

Optimal Universal Quantum Cloning: Asymmetries and Fidelity Measures

Alastair Kay¹

Department of Mathematics, Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK

(Dated: 17 June 2015)

We study the problem of universal quantum cloning – taking several identical copies of a pure but unknown quantum state and producing further copies. While it is well known that it is impossible to perfectly reproduce the state, how well the copies can be cloned can be quantified using the fidelity. We examine how individual fidelities can be traded against each other, and how different fidelity measures can be incorporated. The broadly applicable formalism into which we transform the cloning problem is described as a series of quadratic constraints which are amenable to mathematical and computational scrutiny. As such, we reproduce all known results on optimal universal cloning, and push the recent results on asymmetric cloning much further, giving new trade-off relations between fidelities for broad classes of optimal cloning machines. We also provide substantial evidence that motivates why other parameter ranges (number of input copies) have not, and will not yield to similar analysis.

I. INTRODUCTION

Quantum cloning is the quintessential no-go theorem of quantum mechanics – possible in the classical world, but impossible to implement perfectly in the quantum world, and reflecting such fundamental properties of the quantum world that can be used as a postulate in information theoretic explorations. Ever since the original proofs that an unknown quantum state cannot be perfectly cloned¹, quantifying how well states can be cloned has proved a challenge. When all the clones are required to be the same quality, the achievable qualities are well understood^{2–5}. This covers the case not only of universal cloning, in which the input state is equally likely to be any pure state, but also state-dependent cloning, of qudits⁶. However, asymmetric cloning, when the clones are permitted to have different qualities, has proven far more challenging. Until recently, studies were limited to very specific cases of, for example $1 \rightarrow 3$ universal cloning of qubits^{7,8}, in which one input copy is converted to 3 output copies of differing qualities. However, a recent revelation has permitted calculation of the trade-offs in $1 \rightarrow N$ universal cloning of qudits, for arbitrary N and local Hilbert space dimension $d^{9,10}$. In addition, they revealed a more fundamental insight; there is a direct connection between the ability to share correlations between different spins and the quality of clones that can be produced on those spins. These monogamy-type relationships provide widely applicable bounds for the study of strongly correlated quantum systems, elevating interest in asymmetric cloning beyond that of mathematical curiosity to the foundations of a powerful new calculational tool with properties different to those encapsulated by monogamy of the tangle^{11,12} or of Bell tests¹³, with the added benefit that, by knowing the *optimal* cloning results, these bounds are incredibly stringent.

In this paper, we reproduce the recent calculation for universal asymmetric cloning of qudits^{9,10}, giving full proofs, and expanding the scope of the study to include the cases where multiple copies of a state are provided¹⁰,

and when different measures of the cloning quality are examined. The complete solution to these problems generally requires non-convex optimisation, and can thus be expected to be computationally intractable as the cloning parameters (number of input copies and number of output copies) increase in value.

A. Orientation

This is a mathematically detailed paper and, as such, makes heavy use of specific notation which we will introduce in Section I B. This section could usefully be used as a reference while reading the rest of the document. This is followed by some preliminary properties of the symmetric subspace, and how these properties are altered by the application of the partial transpose operation. These are likely to be familiar to many readers. In Sec. II, we review the Choi-Jamiołkowski isomorphism¹⁴, which is the main technical tool that allows us to give an upper bound on the achievable cloning fidelity by calculating the maximum eigenvalue of a certain matrix. It is then in Section III that we apply this isomorphism to the cloning problem. In particular, we isolate a small subspace of the relevant matrix and use a variant of the Lieb-Mattis theorem (Sec. III B) to show that the maximum eigenvalue of the whole matrix is contained within this subspace¹⁵ and furthermore confirm that the upper bound specified by this formalism can indeed be attained. The resultant problem to be solved consists of a set of quadratic constraints that need to be satisfied.

The following sections are an exploration of the consequences of the developed formalism – Sec. IV completely solves the problem of when $N - 1$ input copies can be transformed into N copies of varying qualities, while Sec. V studies the problem of transforming a single input state into N outputs. In this instance, we reduce the quadratic constraints as far as possible, either by reducing them to linear ones, or by ensuring their convexity. In the cases of primary interest, all non-convex constraints can be elim-

inated, allowing for efficient solution.

The study of different numbers of input copies appears to be far more challenging. Sec. VI proves that if the number of input copies is not 1 or $N - 1$, the problem cannot be reduced to a linear problem, and the task is inherently non-convex. This provides significant insight as to why these cases are far more challenging than those for which a solution has previously been given. Indeed, a solution is not expected (unless $P=NP$).

For completeness, Sec. VIII, gives a partial description of how the optimal asymmetric universal quantum cloner can be realised before we conclude in Sec. IX. Appendix A provides some potentially valuable side results – properties of the key matrices that we do not utilise directly, but could be useful in the future, for improving the implementation protocols for instance.

B. Notation

We will make extensive use of bit strings $x \in \{0, 1\}^N$ (we reserve letters x, y and z for such bit strings). These have a Hamming weight (number of 1 entries) $w_x = x \cdot x$. Typically, we will be using these strings to indicate a subset of spins, so if there are N spins, they are divided into the two sets specified by sites $\{n : x_n = 1\}$ and $\{n : \bar{x}_n = 1\}$ where \bar{x} is the complement of x . As such, we can think about combining sets of sites: $x \cup y$ conveys the set of sites for which either $x_n = 1$ or $y_n = 1$, while $x \cap y$ restricts to those for which $x_n y_n = 1$.

When cloning, we will take M identical input copies, and aim to produce $N > M$ output copies. It is helpful to think of these as two different spaces, the IN space of M spins, and the OUT space of N spins. It is the OUT space that will be subdivided, using bit strings to specify how. The quality of the outputs will be measured by the fidelity (to be defined later), and these fidelities can also be indexed by a bit string y . In the case where the fidelities we are interested in correspond to all the bit strings of weight L , we say that we are examining the (M, L, N) cloning machines.

Definition 1. Define the matrices

$$G_y^{(M)} = \sum_{\substack{z, x \in \{0, 1\}^N \\ w_x = w_z = M}} \frac{|x\rangle \langle z|}{\binom{M+d-1-x \cdot z + w_{x \cap z}}{d-1}}.$$

The M will typically be clear from context and can safely be dropped (there is rarely cause to consider two different values of M simultaneously). d is a positive integer. These may be generalised to

$$G_y^{(M, L)} = \sum_{\substack{x \in \{0, 1\}^N \\ w_x = L \\ x \cdot y = \min(L, w_y)}} G_x^{(M)}.$$

Included in this definition are particularly interesting special cases $G_0^{(M)}$ and $G_0^{(M, L)}$, which have a common

structure that enables simple solution for eigenvalues and eigenvectors (see Appendix A).

We are also interested in the concept of the symmetric subspace.

Definition 2. Let \mathcal{S}_N be the symmetric group on N letters, and $\pi \in \mathcal{S}_N$ be an arbitrary permutation of those letters. The symmetric subspace of a Hilbert space $\mathcal{H} = (\mathbb{C}_d)^{\otimes N}$ is the set of states on \mathcal{H} that are invariant under all such permutations:

$$\mathcal{S}_{\mathcal{H}} := \{|\psi\rangle \in \mathcal{H} : P(\pi)|\psi\rangle = |\psi\rangle \forall \pi \in \mathcal{S}_N\}$$

where $P(\pi)$ is a representation of π on \mathcal{H} .

Definition 3. Projector onto the symmetric subspace:

$$P_{\text{sym}}^N = \frac{1}{n!} \sum_{\pi \in \mathcal{S}_N} P(\pi).$$

In this context, the superscript conveys how many spins the projector acts on. Later, it will also be used to specify which subset of spins it acts on.

To see that this is a projector, note that $P(\pi_1)P(\pi_2) = P(\pi_1\pi_2)$, $\pi_1\pi_2$ is in the group, and the group multiplication is invertible, meaning that $\pi_1\pi_2$ maps to distinct permutations for all π_2 and a fixed π_1 . Hence

$$P_{\text{sym}}^N{}^2 = \frac{1}{n!n!} \sum_{\pi_1 \in \mathcal{S}_N} \sum_{\pi_2 \in \mathcal{S}_N} P(\pi_1) = \frac{1}{n!} \sum_{\pi \in \mathcal{S}_N} P(\pi) = P_{\text{sym}}.$$

Evidently, for any state $|\psi\rangle \in \mathcal{S}_{\mathcal{H}}$, $P_{\text{sym}}|\psi\rangle = |\psi\rangle$, so the span of states that is projected onto certainly includes the symmetric subspace. Furthermore, for any $|\psi\rangle \in \mathcal{H}$ and $\pi \in \mathcal{S}_N$, $P(\pi)P_{\text{sym}}|\psi\rangle = P_{\text{sym}}|\psi\rangle$ because, again, we can fold the $P(\pi)$ into the sum over π in the projector, and this is the definition of a state in $\mathcal{S}_{\mathcal{H}}$. Hence the span of states that is projected onto is a subspace of the symmetric subspace. Taken together, this shows that P_{sym}^N projects onto $\mathcal{S}_{\mathcal{H}}$.

A useful feature of the symmetric subspace is its relation with the spin operators:

Definition 4. For a d -dimensional Hilbert space, we define the following spin operators:

$$\begin{aligned} S^{X,d} &= \sum_{n=1}^{d-1} \sqrt{n(d-n)} (|n-1\rangle \langle n| + |n\rangle \langle n-1|) \\ S^{Y,d} &= \sum_{n=1}^{d-1} i \sqrt{n(d-n)} (|n\rangle \langle n-1| - |n-1\rangle \langle n|) \\ S^{Z,d} &= \sum_{n=0}^{d-1} (d-1-2n) |n\rangle \langle n|, \end{aligned}$$

and in a system composed of the N -fold tensor product of such a Hilbert space, the overall spin operators are

$$J_X = \sum_{n=1}^N \mathbb{1}^{\otimes(n-1)} \otimes S^{X,d} \otimes \mathbb{1}^{\otimes(N-n)}$$

and $J^2 = J_X^2 + J_Y^2 + J_Z^2$.

It is important to note that $[J_Z, J^2] = 0$, so they are simultaneously diagonalisable. We will use $\{|\phi_i^N\rangle\}$ to denote an orthonormal basis for P_{sym}^N , i.e.

$$P_{\text{sym}}^N = \sum_i |\phi_i^N\rangle \langle \phi_i^N|,$$

and will generally assume that the $|\phi_i\rangle$ are also eigenstates of the J_Z operator (for qubits, for example, one can fix that $J_Z |\phi_i^N\rangle = (2i - N) |\phi_i^N\rangle$ for $i = 0, \dots, N$). Alternatively, we will use the superscript to denote the set of spins that the state covers. For instance, we may use $|\phi_i^x\rangle$ to denote a symmetric state of w_x spins located on the sites n specified by $x_n = 1$. It is only a mild abuse of notation to then write $|\phi_i^x\rangle |\phi_j^{\bar{x}}\rangle$ to fully specify the state of N spins. We can also create a Bell state from the symmetric states, defining

$$|B_x^{(M)}\rangle = \frac{1}{\sqrt{\binom{M+d-1}{M}}} \sum_i |\phi_i^{\text{IN}}\rangle |\phi_i^x\rangle$$

for any $x \in \{0, 1\}^N : w_x = M$. Lemma 1 will confirm that this state is correctly normalised.

C. Preliminaries

In this subsection, we review some basic properties of the symmetric subspace¹⁶, and examine the effect of applying the partial transpose operation.

Lemma 1. *The dimension of $S_{\mathcal{H}}$ is $\binom{N+d-1}{N}$.*

Proof. The dimension of the symmetric subspace can be calculated from $\text{Tr}(P_{\text{sym}}^N)$. If we use $[d]$ to denote a choice of labels $1, 2, \dots, d$ then

$$\text{Tr}(P_{\text{sym}}^N) = \frac{1}{n!} \sum_{\pi \in S_N} \sum_{i \in [d]^N} \langle i | P(\pi) | i \rangle.$$

We can consider this sum as, for each i , how many permutations are there that map i to i ? If there are c_1 instances of 1 in i , c_2 of 2 etc. (subject to the constraint $\sum_j c_j = N$), then there are $c_1!$ permutations that map all the 1s back to the 1s. Hence,

$$\text{Tr}(P_{\text{sym}}^N) = \frac{1}{N!} \sum_{i \in [d]^N} \prod_{j=1}^N c_j!.$$

But, of all the strings i , how many have c_1 1s, c_2 2s etc? $\frac{N!}{\prod_{j=1}^N c_j!}$. This leaves us needing to know the number of distinct configurations of the $\{c_j\}$ that are possible, i.e. how many ways are there to distribute N indistinguishable items between d bins? $\binom{N+d-1}{N}$. \square

Lemma 2. *The operator defined on M input qubits and w output qubits by*

$$\rho_{\text{IN}, \text{OUT}} := \int (U^* |0\rangle \langle 0| U^T)^{\otimes M} \otimes (U |0\rangle \langle 0| U^\dagger)^{\otimes w} dU,$$

with integration being taken uniformly over the Haar measure for $U \in SU(d)$, satisfies

$$\rho_{\text{IN}, \text{OUT}}^{T_{\text{IN}}} = \frac{P_{\text{sym}}^{M+w}}{\binom{M+w+d-1}{M+w}}.$$

T_{IN} denotes the partial transpose over the M input spins.

Proof. If we take the partial transpose, we have that

$$\rho_{\text{IN}, \text{OUT}}^{T_{\text{IN}}} = \int (U |0\rangle \langle 0| U^\dagger)^{\otimes (M+w)} dU.$$

This is clearly a mixture of all possible states $|\psi\rangle \langle \psi|^{\otimes (M+w)}$, which is the symmetric subspace, we just have to be careful with the normalisation. The trace is unaffected by partial transpose operations, so given that $\text{Tr}(\rho_{\text{IN}, \text{OUT}}) = 1$ and, by Lemma 1,

$$\text{Tr}(P_{\text{sym}}^{M+w}) = \binom{M+w+d-1}{M+w},$$

we have the desired result. \square

Corollary 1. *The matrix elements of ρ are non-negative.*

Proof. An element $N! \langle i | P_{\text{sym}}^N | j \rangle$ counts the permutations that map the string i in to the string j . This is clearly non-negative. The partial transpose rearranges matrix elements and does not change their values. \square

Lemma 2 contains the statement of twirling¹⁷ as a special case (with, perhaps, a more straightforward proof):

Corollary 2. *For $M = w = 1$, $\rho = \frac{|B^{(1)}\rangle \langle B^{(1)}|}{d+1} + \frac{1}{d(d+1)}$.*

Proof. The basis elements of the symmetric subspace of a $d \times d$ Hilbert space consist of $|ii\rangle$ and $(|ij\rangle + |ji\rangle)/\sqrt{2}$ for $i \neq j$.

$$P_{\text{sym}}^2 = \sum_{i=0}^{d-1} |ii\rangle \langle ii| + \frac{1}{2} \sum_{i \neq j} (|ij\rangle + |ji\rangle)(\langle ij| + \langle ji|),$$

so

$$\begin{aligned} \rho_{1,1} &= \frac{2}{d(d+1)} P_{\text{sym}}^{T_{\text{IN}}} \\ &= \frac{2 \sum_i |ii\rangle \langle ii| + \sum_{i \neq j} (|ij\rangle \langle ij| + |ji\rangle \langle ji| + |ii\rangle \langle jj| + |jj\rangle \langle ii|)}{d(d+1)} \\ &= \frac{1}{d(d+1)} + \frac{|B^{(1)}\rangle \langle B^{(1)}|}{d+1}. \end{aligned}$$

\square

Lemma 3. *The matrix ρ satisfies*

$$\begin{aligned} [\rho, (U_I^{\otimes M} \otimes \mathbb{1}^{\otimes w}) J_Z (U_I^{\dagger \otimes M} \otimes \mathbb{1}^{\otimes w})] &= 0 \\ [\rho, (U_I^{\otimes M} \otimes \mathbb{1}^{\otimes w}) J^2 (U_I^{\dagger \otimes M} \otimes \mathbb{1}^{\otimes w})] &= 0 \end{aligned}$$

where $U_I = \sum_{n=0}^{d-1} (-1)^n |n\rangle \langle d-1-n|$.

Proof. It is clear that $[P_{\text{sym}}^{M+w}, J_Z] = 0$ (and for J_X, J_Y) and $[P_{\text{sym}}^{M+w}, J^2] = 0$ given that the total spin operators are invariant under permutations of underlying spins. Now, divide the sum for J_Z (for instance) into a sum over terms on the input space, and terms on the output space. It must be that

$$[P_{\text{sym}}^{M+w}, \sum_{\text{IN}} S^Z + \sum_{\text{OUT}} S^Z] = 0,$$

so we take the partial transpose over the input spins:

$$[\rho_{M,w}, -\sum_{\text{IN}} S^{Z^T} + \sum_{\text{OUT}} S^Z] = 0.$$

The - sign appears due to the change in ordering of operators under the action of the transpose. Furthermore,

$$-S_Z^T = -S_Z \quad -S_X^T = -S_X \quad -S_Y^T = S_Y,$$

so provided we can find a unitary U_I that maps $S_Z \mapsto -S_Z$, $S_X \mapsto -S_X$ and $S_Y \mapsto S_Y$, it must be that

$$[\rho, (U_I^{\otimes M} \otimes \mathbb{1}^{\otimes w} J_Z U_I^{\dagger \otimes M} \otimes \mathbb{1}^{\otimes w})] = 0.$$

The specified U_I achieves this. \square

Lemma 4. For any $d \times d$ matrix M

$$M^T \otimes \mathbb{1} \left| B^{(1)} \right\rangle = \mathbb{1} \otimes M \left| B^{(1)} \right\rangle.$$

The proof of this is a simple case of explicitly writing $M = \sum_{i,j} M_{i,j} |i\rangle \langle j|$ and verifying the equivalence. It is left to the reader.

II. THE CHOI-JAMIOŁKOWSKI ISOMORPHISM

The scenario is that, given one of a set of states $|\psi_i\rangle$ ($i = 1, \dots, K$), we are required to perform a particular state transformation on it, without being told which of the states we have been given. The required transformation may not be achievable exactly within the quantum formalism, but is best approximated within the theory by a completely positive, trace preserving map \mathcal{E} that transforms input state $|\psi_i\rangle$ into $\mathcal{E}(|\psi_i\rangle)$. The success of the state transformation task is then measured by a fidelity given by

$$F = \frac{1}{K} \sum_i \text{Tr}(\mathcal{M}_i \mathcal{E}(|\psi_i\rangle)).$$

Here \mathcal{M}_i are positive operators ($\mathcal{M}_i \geq 0$) satisfying $\|\mathcal{M}_i\| \leq 1$ so that F is indeed a fidelity taking values between 0 and 1. If the fidelity takes value 1, we infer that the map has perfectly implemented the required state transformation for all the specified input states. As a simple example, consider being required to transform the states $|\psi_i\rangle$ into states $|\phi_i\rangle$, in which case we simply

define $\mathcal{M}_i = |\phi_i\rangle \langle \phi_i|$. For a continuous set of states, the sum appearing in the definition of F transforms to an integral. The factor of $1/K$ appearing in the definition stems from the assumption that each of the input states $|\psi_i\rangle$ is equally likely. If this is not the case, these parameters can be adjusted based on a given probability distribution of the input states.

Lemma 5. For the state transformation task, the achievable fidelity is upper bounded by the maximum eigenvalue of the operator

$$R = \frac{d'}{K} \sum_i |\psi_i\rangle \langle \psi_i|_I^T \otimes \mathcal{M}_i, \quad (1)$$

where d' is the dimension of the subspace spanned by the states $\{|\psi_i\rangle\}$.

Proof. We start by introducing a Hilbert space of two parts, an input space and an output space, both of dimension d , the dimension of the Hilbert space from which the $|\psi_i\rangle$ are taken, and consider the maximally entangled state $|\Psi\rangle_{IO}$ between them, as applies only to the subspace of states $\{|\psi_i\rangle\}$. This lets us rewrite $|\psi\rangle \langle \psi|_{\text{OUT}} = d' \text{Tr}_{\text{IN}}(|\psi\rangle \langle \psi|^T \otimes \mathbb{1} \cdot |\Psi\rangle \langle \Psi|)$ using Lemma 4. So,

$$F = \frac{d'}{K} \sum_i \text{Tr} \left(|\psi\rangle \langle \psi|^T \otimes \mathcal{M}_i \cdot (\mathbb{1} \otimes \mathcal{E})(|\Psi\rangle \langle \Psi|) \right).$$

Since \mathcal{E} is a completely positive operator, its extension is well defined, and we can let $\chi = (\mathbb{1} \otimes \mathcal{E})(|\Psi\rangle \langle \Psi|)$. The trace preserving property of \mathcal{E} imposes that $\text{Tr}(\chi) = \text{Tr}|\Psi\rangle \langle \Psi| = 1$ (if it weren't trace preserving, we would have $\text{Tr}(\chi) \leq 1$, which doesn't change our conclusion). So, $F = \text{Tr}(R\chi) \leq \lambda \text{Tr}(\chi) \leq \lambda$ where λ is the maximum eigenvalue of R , and χ is the corresponding (normalised) maximum eigenvector. \square

The above proof does not guarantee that a map described by state χ can be implemented; that is the purpose of the following Lemma.

Lemma 6. The upper bound for the achievable fidelity in the state transformation task can be realised if there exists a mixture ρ of the maximum eigenvectors of R such that $\text{Tr}_{\text{OUT}}(\rho) = \mathbb{1}/d'$, where $\mathbb{1}$ is over the subspace spanned by the states $\{|\psi_i\rangle\}$. If ρ is a pure state, then the cloning can be achieved economically.

Proof. Let the maximum eigenvector of R be $|\chi\rangle$. For any choice of $|\chi\rangle$ (allowing for the fact that the maximum eigenvalue may be degenerate), it can be expressed as a pure bipartite state between the subsystems IN and OUT with a Schmidt decomposition

$$|\chi\rangle = \sum_{n=0}^{d-1} \beta_n |\eta_n\rangle |\lambda_n\rangle,$$

where $\{|\eta_n\rangle\}$ define an orthonormal basis over the d' dimensional Hilbert space. If there exists a maximum eigenvector such that $\beta_n^2 = \frac{1}{d'}$, then

$$d' \text{Tr}_{\text{IN}}(|\psi\rangle\langle\psi|^T \otimes \mathbb{1} |\chi\rangle\langle\chi|) = U |\psi\rangle\langle\psi| U^\dagger$$

where

$$U |\eta_n\rangle = |\lambda_n\rangle \quad \forall n \in [d'].$$

Here the relevant Hilbert spaces are extended as necessary so that they have the same size. In this instance, the optimal strategy (application of U to the input state) is called economical, meaning that one does not require an ancilla for the operation to be implemented.

If this cannot be done, but there exists a mixture of maximum eigenvectors such that $\text{Tr}_{\text{OUT}}(\rho) = 1/d'$, then it is always possible to introduce an ancillary system of Hilbert space no larger than d'^2 that purifies ρ and gives Schmidt coefficients between the system IN and the rest of value $1/d'$. By the previous argument, we can therefore implement a unitary operation over this extended space (meaning it is no longer economical) that realises the desired map. \square

III. CLONING

We study the $M \rightarrow N$ universal cloning problem. This means that we are given M copies of an unknown pure state, and are tasked with making $N > M$ copies of it, as well as we can. Universal cloning imposes that the unknown quantum state is drawn uniformly from all possible pure states (i.e. $U|0\rangle$ where U is drawn uniformly over $SU(d)$). Most studies concentrate on symmetric cloning, in which we want all of the copies produced to be as good as each other. Here, we aim for the loftier goal of wanting to know how we can trade the qualities of the different outputs. Traditionally, one concentrates on the single-clone fidelity:

$$M(\psi) = \sum_{n=1}^N \alpha_n \mathbb{1}^{\otimes(n-1)} \otimes |\psi\rangle\langle\psi| \otimes \mathbb{1}^{\otimes(N-n)},$$

where $\alpha_n \geq 0$ ensures positivity, and $\sum_n \alpha_n = 1$ ensures that the maximum value is 1, which only happens for the state $|\psi\rangle^{\otimes N}$. This lets us examine the individual copies. However, other measures have been considered, such as the global fidelity:

$$M(\psi) = |\psi\rangle\langle\psi|^{\otimes N}.$$

We aim to consider a fully general case where we evaluate the fidelities on arbitrary subsets of qubits. This will be specified by $\Lambda \subseteq \{0,1\}^N$, meaning that any $x \in \Lambda$ wants us to evaluate the fidelity across all sites n for which $x_n = 1$, and not over the sites $x_n = 0$. As such, we can take

$$M(\psi) = \sum_{x \in \Lambda} \alpha_x \bigotimes_{n=1}^N |\psi\rangle\langle\psi|^{x_n}$$

where $\sum_{x \in \Lambda} \alpha_x = 1$ (and by $|\psi\rangle\langle\psi|^0$ we understand $\mathbb{1}$). We use a shorthand of $|\psi\rangle\langle\psi|_x \otimes \mathbb{1}_{\bar{x}}$ to describe the tensor product $\bigotimes_{n=1}^N |\psi\rangle\langle\psi|^{x_n}$.

According to Lemma 5, our task is to find the maximum eigenvalue λ and eigenvector $|\chi\rangle$ of the matrix

$$R = \sum_{x \in \{0,1\}^N} \alpha_x R_x$$

where

$$\begin{aligned} R_x &= d' \int |\psi\rangle\langle\psi|_{\text{IN}}^T \otimes |\psi\rangle\langle\psi|_x \otimes \mathbb{1}_{\bar{x}} d\psi \\ &= d' \int (U|0\rangle\langle 0|U^\dagger)_{\text{IN}}^T \otimes (U|0\rangle\langle 0|U^\dagger)_x \otimes \mathbb{1}_{\bar{x}} dU. \end{aligned}$$

The realised fidelity $F = \lambda$ can be described by $\sum_x \alpha_x F_x$ where F_x is the fidelity of the set of clones at the sites $x_n = 1$: $F_x = \langle\chi| R_x |\chi\rangle$. By Lemma 2,

$$R_x^{\text{IN}} = \frac{\binom{M+d-1}{M}}{\binom{M+w_x+d-1}{M+w_x}} P_{\text{sym}}^{M+w_x}.$$

We know from Lemma 3 that $R = \sum_x \alpha_x R_x$ simultaneously commutes with both J^2 and J_Z (up to a unitary rotation), and it therefore has two quantum numbers S (where $4S(S+1)$ is an eigenvalue of J^2) and M_Z (taking values $-S$ to S in integer steps) that distinguish subspaces of eigenvectors.

Definition 5. We denote by $|\psi_x\rangle$ for $x \in \{0,1\}^N$ and $w_x = M$ the state $|B_x^{(M)}\rangle |\Phi\rangle_{\bar{x}}$, where $|\Phi\rangle$ is a symmetric state of the $N - M$ spins on \bar{x} .

Lemma 7. Let $x, y \in \{0,1\}^N$ where $w_y = M$. The state

$$|\eta_{x,y}\rangle = \sqrt{\frac{\binom{M+d-1}{M} \binom{w_x - x \cdot y + d - 1}{d-1}}{\binom{w_x + M - x \cdot y + d - 1}{d-1}}} \mathbb{1}_{\text{IN}} \otimes P_{\text{sym}}^{x \cup y} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} |\psi_y\rangle,$$

is correctly normalised.

Proof. Rewriting the projection operator as the integral,

$$P_{\text{sym}}^{x \cup y} = \binom{w_x + M - x \cdot y + d - 1}{d-1} \int (U|0\rangle\langle 0|U^\dagger)^{\otimes(w_x + M - x \cdot y)} dU,$$

we have that

$$\langle \eta_{x,y} | \eta_{x,y} \rangle = \binom{M+d-1}{M} \binom{w_x - x \cdot y + d - 1}{d-1} \text{Tr} \left(\int \left| B_y^{(M)} \right\rangle \left\langle B_y^{(M)} \right| \otimes |\Phi\rangle \langle \Phi|_{\bar{y}} \cdot \mathbb{1}_{\text{IN}} \otimes (U |0\rangle \langle 0| U^\dagger)^{\otimes (w_x + M - x \cdot y)} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} dU \right).$$

However, for the spins where $y_n = 1$, we can absorb the U s into the $\left| B_y^{(M)} \right\rangle$ (U_y acts as a unitary within the symmetric subspace of spins $y_n = 1$): $\mathbb{1}_{\text{IN}} \otimes U_y \left| B_y^{(M)} \right\rangle = U_{\text{IN}}^* \otimes \mathbb{1}_y \left| B_y^{(M)} \right\rangle$ by Lemma 4, and they cancel, leaving

$$\begin{aligned} \langle \eta_{x,y} | \eta_{x,y} \rangle &= \binom{M+d-1}{M} \binom{w_x - x \cdot y + d - 1}{d-1} \text{Tr} \left(\int \left| B_y^{(M)} \right\rangle \left\langle B_y^{(M)} \right| \otimes |\Phi\rangle \langle \Phi| \cdot \mathbb{1}_{\text{IN}} \otimes |0\rangle \langle 0|_y \otimes (U |0\rangle \langle 0| U^\dagger)_{\otimes (x \cap \bar{y})} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} dU \right) \\ &= \binom{w_x - x \cdot y + d - 1}{d-1} \text{Tr} \left(\int |\Phi\rangle \langle \Phi| \cdot (U |0\rangle \langle 0| U^\dagger)_{x \cap \bar{y}} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} dU \right) \\ &= \text{Tr} \left(|\Phi\rangle \langle \Phi| \cdot P_{\text{sym}}^{x \cap \bar{y}} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} \right) \end{aligned}$$

Since $|\Phi\rangle$ is a +1 eigenstate of all possible permutations of its spins, this includes the permutations involved on the subset of spins $x \cap \bar{y}$. Thus, the trace has value 1 and we are left with $\langle \eta_{x,y} | \eta_{x,y} \rangle = 1$. \square

Lemma 8. *For any two binary strings $x, y \in \{0, 1\}^N$ with $w_x = w_y = M$,*

$$\langle \psi_x | \psi_y \rangle = \frac{1}{\binom{M - x \cdot y + d - 1}{d-1}}.$$

Proof. Clearly, the value $\langle \psi_x | \psi_y \rangle$ will only depend on the value $x \cdot y$, and not on the specific choices of x and y . We will prove the value by induction. As a base case, take $x \cdot y = M$, i.e. $x = y$. Evidently, $\langle \psi_x | \psi_y \rangle = 1$, as predicted. For the inductive step, assume this formula holds for all values of $x \cdot y = k + 1, \dots, M$, and we aim to show that it holds for $x \cdot y = k$.

Select x and y such that $x \cdot y = k$. Now consider the state $|\eta_{x,y}\rangle$ of Lemma 7. We have that

$$|\eta_{x,y}\rangle = \sqrt{\frac{\binom{M+d-1}{M} \binom{M-k+d-1}{d-1}}{\binom{2M-k+d-1}{d-1}}} \frac{1}{\binom{2M-k}{M}} \sum_{\substack{z \in \{0,1\}^N \\ w_z = M \\ z \cdot (x \cup y) = M}} |\psi_z\rangle.$$

From Lemma 7, $\langle \eta_{x,y} | \eta_{x,y} \rangle = 1$. So, taking the inner

product gives

$$\frac{\binom{2M-k}{M} \binom{w_x + M - x \cdot y + d - 1}{d-1}}{\binom{M+d-1}{M} \binom{w_x - x \cdot y + d - 1}{d-1}} = \binom{M}{k} \langle \psi_x | \psi_y \rangle + \sum_{q=k+1}^M \frac{\binom{M}{q} \binom{M-k}{M-q}}{\binom{M-q+d-1}{d-1}},$$

where we have used the inductive assumption to give the denominator of the final term. Hence,

$$\frac{\binom{2M-k+d-1}{M}}{\binom{M+d-1}{M}} = \binom{M}{k} \left(\langle \psi_x | \psi_y \rangle - \frac{1}{\binom{M-k+d-1}{d-1}} \right) + \frac{\binom{2M-k+d-1}{M}}{\binom{M+d-1}{M}}.$$

Rearranging gives the desired result:

$$\langle \psi_x | \psi_y \rangle = \frac{1}{\binom{M-k+d-1}{d-1}}.$$

\square

Lemma 9. *The states $\mathcal{S}_{\text{special}} := \{|\psi_y\rangle\}$ define a closed subspace under the action of $\{R_x\}$. By fixing a J_Z subspace for the symmetric state $|\Phi\rangle$, $\mathcal{S}_{\text{special}}$ is a subspace of fixed quantum number M_Z .*

Proof. The previous Lemma conveyed that $|\eta_{x,y}\rangle$ is supported on $\mathcal{S}_{\text{special}}$. We now claim that $|\tilde{\eta}\rangle = |\eta_{x,y}\rangle$ where

$$|\tilde{\eta}\rangle := \frac{\sqrt{\binom{M+d-1}{M} \binom{w_x - x \cdot y + d - 1}{d-1} \binom{w_x + M - x \cdot y + d - 1}{d-1}}}{\binom{M+w_x+d-1}{d-1}} P_{\text{sym}}^{\text{IN}, x T_{\text{IN}}} |\psi_y\rangle,$$

i.e. we aim to show that $\langle \tilde{\eta} | \tilde{\eta} \rangle = 1$ and $\langle \tilde{\eta} | \eta \rangle = 1$.

$$\frac{\langle \tilde{\eta} | \tilde{\eta} \rangle}{\binom{w_x - x \cdot y + d - 1}{d-1} \binom{w_x + M - x \cdot y + d - 1}{d-1} \binom{M+d-1}{M}} = \iint \langle \psi_y | (U^* |0\rangle \langle 0| U^T V^* |0\rangle \langle 0| V^T)_{\text{IN}} \otimes (U |0\rangle \langle 0| U^\dagger V |0\rangle \langle 0| V^\dagger)_{x \otimes \mathbb{1}_{\bar{x}}} |\psi_y\rangle dU dV$$

Moving the unitaries through the states $|\Psi\rangle$ where possible, this reduces to

$$\frac{\langle \tilde{\eta} | \tilde{\eta} \rangle}{\binom{w_x - x \cdot y + d - 1}{d-1} \binom{w_x + M - x \cdot y + d - 1}{d-1}} = \iint \langle \Phi |_{\bar{y}} (U |0\rangle \langle 0| U^\dagger V |0\rangle \langle 0| V^\dagger)_{x \cap \bar{y}} \otimes \mathbb{1}_{\bar{x} \cap \bar{y}} |\Phi\rangle_{\bar{y}} \langle 0| U^\dagger V |0\rangle^{M+w_x-x \cdot y} \langle 0| U^T V^* |0\rangle^M dU dV$$

We substitute $W = U^\dagger V$ (eliminating V) and integrate

over U , giving

$$\begin{aligned} \langle \tilde{\eta} | \tilde{\eta} \rangle &= \binom{w_x + M - x \cdot y + d - 1}{d-1} \int |\langle 0 | W | 0 \rangle|^{2(M+w_x-x \cdot y)} dW \\ &= 1 \end{aligned}$$

Calculation of $\langle \eta | \tilde{\eta} \rangle$ follows an identical trajectory, yielding the desired result. \square

We therefore see that there are many degenerate spaces (different choices of the state $|\Phi\rangle$), and eigenvectors within these subspaces can be described by states

$$|\chi\rangle = \sum_{\substack{x \in \{0,1\}^N \\ w_x = M}} \beta_x |\psi_x\rangle$$

for coefficients $\{\beta_x\}$ which are normalised as

$$\sum_{x,z} \frac{\beta_x \beta_z}{\binom{M-x \cdot z + d-1}{d-1}} \leq 1 \quad \Leftrightarrow \quad \underline{\beta}^T G_0^{(M)} \underline{\beta} \leq 1$$

by Lemma 8. Here we have grouped all the parameters β_x into a single vector $\underline{\beta}$. Each of the individual fidelities $F_y = \langle \chi | R_y | \chi \rangle$ can be evaluated as

$$\langle \chi | R_y | \chi \rangle = \binom{M+d-1}{M} \sum_{\substack{x,z \in \{0,1\}^N \\ w_x = w_z = M}} \beta_x \beta_z \frac{\langle \psi_x | P_{\text{sym}}^{\text{IN},y T_{\text{IN}}} | \psi_z \rangle}{\binom{M+w_y+d-1}{d-1}}$$

By Lemma 9, this simplifies to

$$F_y = \underline{\beta}^T G_y^{(M)} \underline{\beta}.$$

Note that in the next section we will prove that the maximum eigenvector will correspond to all the entries $\beta_x \geq 0$, so we can use $\underline{\beta}^T$ instead of $\underline{\beta}^\dagger$ without loss of generality.

A. Example: Symmetric Cloning

Consider the case of symmetric cloning, in which we demand that all fidelities be measured on the same number of spins (say L) and that all fidelities be the same, which is achieved by setting $\alpha_x = \frac{1}{\binom{N}{L}}$ for all x . We thus want to find the maximum eigenvalue of the matrix

$$\frac{1}{\binom{N}{L}} \sum_{y: w_y = M} G_y^{(M)} = \frac{1}{\binom{N}{L}} G_0^{(M,L)}.$$

This matrix has the structure that all of the rows are just permutations of each other, and all the matrix elements are positive. Hence, the maximum eigenvector is just the uniform superposition of all possible basis states, and the eigenvalue is equal to the row sum. In Appendix A, we show that this calculation is given by

$$\frac{1}{\binom{N}{L}} \sum_{i=0}^M \binom{M}{i} \binom{N-M}{M-i} \sum_{q=0}^{N+i-2M} \frac{\binom{N+i-2M}{q} \binom{2M-i}{L-q}}{\binom{M+d-1-i+q}{d-1}},$$

except that we must remember to take into account the normalisation of the state. Hence,

$$F = \frac{1}{\binom{N}{L}} \frac{\binom{M+d-1}{M}}{\binom{N+d-1}{M}} \sum_{i=0}^M \binom{M}{i} \binom{N-M}{M-i} \sum_{q=0}^{N+i-2M} \frac{\binom{N+i-2M}{q} \binom{2M-i}{L-q}}{\binom{M+d-1-i+q}{d-1}}, \quad (2)$$

which simplifies to

$$F = \frac{1}{\binom{N}{L} \binom{N+d-1}{N-M}} \sum_{i=0}^M \sum_{q=0}^N \binom{M}{i} \binom{q-M}{i} \binom{N-M+d-1}{N-q} \binom{M+i}{q-L}. \quad (3)$$

In the special case of $L = 1$, the sum over q in Eqn. (2) is restricted between 0 and 1, giving

$$F = \frac{M}{N} + \frac{(N-M)(M+1)}{N(M+d)},$$

which coincides with the standard result^{3,6}. In the case of $L = N$, the sum in Eqn. (3) is restricted to $q = N$, giving the known result for the global fidelity,

$$F = \frac{\binom{M+d-1}{M}}{\binom{N+d-1}{N}}.$$

Wang et al.¹⁸ claim the general formula of

$$F = \sum_{q=0}^N \frac{\binom{q}{M} \binom{q}{L} \binom{N-q+d-2}{d-2}}{\binom{N}{L} \binom{N+d-1}{N-M}}$$

although we have been unable to prove equivalence with Eq. (3) beyond special cases and numerical tests.

1. Simplified Fidelity Tests

The symmetric cloner already provides a simple test for whether certain cloning tasks are achievable or not. Given that we are asking whether there exists a suitably normalised vector such that

$$F_y \leq \beta^T G_y^{(M)} \beta \quad \forall y : w_y = L,$$

then by summing these, we have

$$\sum_{y: w_y = L} F_y \leq \beta^T G_0^{(M,L)} \beta \leq \binom{N}{M} F_{\text{sym}}.$$

So, if this inequality is violated, cloning must be impossible regardless of the asymmetry. Obviously, this is tight at the point of perfect symmetry, and will be a good approximation close to that point. Also, simple considerations in the case study of Appendix B suggest that it could often be the case for non-trivial M that the bound is tight over much broader ranges. Evidently, satisfying the constraint can never be sufficient proof that cloning is possible as it disguises all the subtleties of the desired asymmetries. As a clear example, consider $3 \rightarrow 4$ cloning with the $L = 2$ fidelity. It is possible to achieve 3 fidelities all being 1 (e.g. $F_{1100}, F_{0110}, F_{1010}$) because this just corresponds to perfect teleportation from the input spins to the first 3 output spins. Whereas, demanding $F_{1100} = F_{0011} = F_{1010} = 1$ will clearly be impossible and yet it could still have the same total fidelity, see Fig. 1.

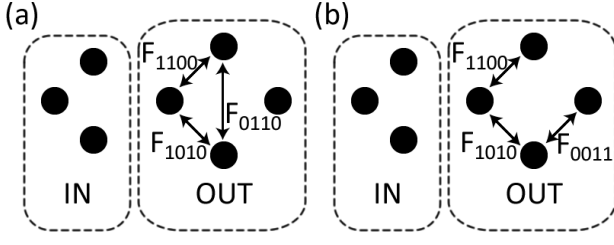


FIG. 1. When tasked with converting 3 identical input states into 4 copies, it is possible to get 3 copies perfectly, and hence certain subsets of 2-copy fidelities can all be 1 (a). Meanwhile, other subsets (b) would require every copy to be identical to the input state, which is clearly impossible.

B. Lieb-Mattis Theorem

So far, we have demonstrated that in the task of finding the optimal cloning fidelity, we can give an upper bound by finding the maximum eigenvalue of the matrix R . We have explored an explicit parametrisation for the maximum eigenvector within a particular subspace, so it remains to prove that the subspace $\mathcal{S}_{\text{special}}$ contains the maximum eigenvector of R , and that this fidelity can be achieved. We do this by introducing a modified version of the Lieb-Mattis Theorem¹⁵.

Lemma 10. *The maximum eigenvector of R within a given M_Z subspace has non-negative coefficients on all the basis states.*

Proof. Divide R into two components, the diagonal elements (R_d) and the remaining, off-diagonal, elements (R_o). In the computational basis, $|a\rangle$, we have $\langle a|R_d|a\rangle = e_a$ and $\langle a|R_o|b\rangle = K_{ab}$. Note that $K_{ab} \geq 0$ by Corollary 1. Assume that in a particular excitation subspace, M_Z , we know the maximum eigenvector,

$$|\chi\rangle = \sum_a f_a |a\rangle,$$

with eigenvalue E_{M_Z} . Hence,

$$\sum_b K_{ba} f_b = (E_{M_Z} - e_a) f_a.$$

Any other state must have a smaller expectation value of R , unless it is also a maximum eigenvector. Let us first try a state $|a\rangle$ as the ansatz. This reveals $e_a \leq E_{M_Z}$. Hence, we can take the modulus of the above equation,

$$\left| \sum_b K_{ba} f_b \right| = (E_{M_Z} - e_a) |f_a|.$$

Next, consideration of the ansatz state

$$|\tilde{\chi}\rangle = \sum_a |f_a| |a\rangle$$

imposes that there is at least one non-zero f_a such that

$$\sum_b K_{ba} |f_b| \leq (E_{M_Z} - e_a) |f_a|$$

but since $\sum_b K_{ba} |f_b| \geq |\sum_b K_{ba} f_b|$, this can only be satisfied with equality for every a , meaning that, up to a global phase factor, the coefficients of the maximum eigenvector in each M_Z subspace satisfy

$$f_a \geq 0.$$

□

Corollary 3. *The maximum eigenvector of R is contained within the span of states of $\mathcal{S}_{\text{special}}$.*

Proof. Consider the state $|\chi_{\text{sym}}\rangle$ for which all the β_x are chosen to be equal, and the state $|\Phi\rangle$ is chosen to be the uniform superposition of all basis states of $N - M$ spins within a fixed M_Z subspace (total excitation number). Overall, this state contains all basis states $|a\rangle |b\rangle$ for $a \in \{0, 1\}^M$ and $b \in \{0, 1\}^N$ provided a exists as a subset of b , for a fixed value of $M_Z = M_Z(b) - M_Z(a)$, and has a positive amplitude on all such states. Note that the remaining basis states cannot contribute to the optimal cloner: the output of the cloning map, $|b\rangle$, when applied to an input $|a\rangle$, would be orthogonal to the input for all possible clones. We can therefore discount these states¹⁹. If the maximum eigenvector for a given M_Z has all non-negative coefficients, it must have non-zero overlap with the appropriate $|\chi_{\text{sym}}\rangle$, which has support on $\mathcal{S}_{\text{special}}$. The only way that this can happen is if the maximum eigenvector is in the space $\mathcal{S}_{\text{special}}$.

This establishes that for the subspaces $M_Z = -\frac{1}{2}(d-1)(N-M), \dots, \frac{1}{2}(d-1)(N-M)$, we can find the maximum eigenvector. The maximum eigenvector in the other subspaces cannot have a larger eigenvalue – if it were true that these other subspaces had an eigenvector with a larger eigenvalue, then this eigenvector must be drawn from a subspace of $S > \frac{1}{2}(d-1)(N-1)$. However, any such eigenvalue is degenerate in M_Z so it would also be present in all other M_Z subspaces from $-S$ to S , in particular in the ones in which we have already found a different maximum eigenvector. □

In principle, we now have an upper bound on the cloning fidelity. Can this be achieved? We invoke Lemma 6, where, although the coefficients $\{\beta_x\}$ are fixed, we are free to pick $|\Phi\rangle$ to be an arbitrary symmetric state, or a mixture thereof.

Lemma 11. *For the upper bound on the cloning fidelity to be achievable, we require a symmetric state $|\Phi\rangle$ of $N - M$ spin d systems, or mixture thereof, such that*

$$\text{Tr}_{M+1, \dots, N-M} |\Phi\rangle \langle \Phi| = \frac{P_{\text{sym}}^M}{\binom{M+d-1}{M}}.$$

Proof. Since we require

$$\text{Tr}_{\text{OUT}} |\chi\rangle \langle \chi| = \frac{1}{\binom{M+d-1}{M}} \sum_i \left| \phi_i^{(M)} \right\rangle \left\langle \phi_i^{(M)} \right|,$$

or that there exists a mixture of such states

$$\sum_{\Phi} p_{\Phi} \text{Tr}_{\text{OUT}} |\chi(\Phi)\rangle \langle \chi(\Phi)| = \frac{1}{\binom{M+d-1}{M}} \sum_i \left| \phi_i^{(M)} \right\rangle \left\langle \phi_i^{(M)} \right|,$$

and recalling that all of the matrix elements are non-negative, we require that each $\text{Tr}_{\text{OUT}} |\chi(\Phi)\rangle \langle \chi(\Phi)|$ is diagonal on the symmetric subspace, i.e. $\langle \lambda_i | \lambda_j \rangle = 0$ for $i \neq j$ where

$$|\lambda_i\rangle = \sum_x \beta_x |\phi_i^x\rangle |\Phi\rangle_{\bar{x}}.$$

When starting to calculate $\langle \lambda_i | \lambda_j \rangle$, it is important to recall the permutation invariance of each $|\phi_i^{(M)}\rangle$ such that, if we can separate out a single qubit such as $|\phi_i^{(M)}\rangle = \sum \alpha_j |j\rangle |\varphi_j\rangle$, then it doesn't matter which spin we pick – the decomposition is always the same. This lets us relate

$$\langle \lambda_i | \lambda_j \rangle = \left\langle \phi_i^{(M)} \right| \text{Tr}_{N-2M+x \cdot z} (|\Phi\rangle \langle \Phi|) \otimes \mathbb{1}_{x \cdot z} \left| \phi_j^{(M)} \right\rangle,$$

and when considering the mixture, fixes that

$$\sum p_{\Phi} \langle \lambda_i(\Phi) | \lambda_j(\Phi) \rangle = \frac{\delta_{i,j}}{\binom{M+d-1}{M}}.$$

We have dropped an explicit enumeration of which spins the states apply to because this purely mathematical manipulation has removed such a direct connection, and the partial trace is thus just taken over any set of $N - 2M + x \cdot z$ spins. This must be true for all values of $x \cdot z = 0, 1, \dots, M$ and for all $i = 0, 1, \dots, \binom{M+d-1}{M}$, which in turn imposes that

$$\text{Tr}_{N-M-k} \left(\sum p_{\Phi} |\Phi\rangle \langle \Phi| \right) = \frac{P_{\text{sym}}^k}{\binom{k+d-1}{k}}$$

for $k = 0, 1, \dots, M$. However, if it is true for $k = M$, it is true for all those values. \square

Corollary 4. *The optimal cloning fidelity can always be achieved. A necessary condition for economical cloning to be achievable is $N \geq 3M$.*

Proof. We can pick a mixture of symmetric states

$$\frac{P_{\text{sym}}^{N-M}}{\binom{N-M+d-1}{d-1}},$$

which clearly satisfies the condition of Lemma 11, so we can certainly always realise uneconomical cloning. For economy, we demand the existence of a pure state. However, consider the Schmidt decomposition of any such

state when the spins are split into a bipartition of M vs. $N - 2M$, giving the partial trace required by Lemma 11. This means that the dimension of the symmetric subspace of the remaining $N - 2M$ spins must be at least $\binom{M+d-1}{M}$, i.e. $N \geq 3M$. \square

A trivial example is the case of $M = 1$. We now know that an ancilla, often known as an ‘anti-clone’²⁰, is required for $N = 2$. For $N \geq 3$, we have to find a symmetric state that has partial trace on a single spin of the maximally mixed state. This is easily achieved with

$$\frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes (N-M)}.$$

Such choices are not unique²¹. Nevertheless, it seems that economical cloning is an unusual property. For $d = 2$, we can construct states for $M = 2, 3$ and $N = 3M$. For instance,

$$\sqrt{3} |\Phi\rangle = |00\rangle \frac{|01\rangle + |10\rangle}{\sqrt{2}} + \frac{|01\rangle + |10\rangle}{\sqrt{2}} |00\rangle + |11\rangle |11\rangle$$

is permutation invariant and has the requisite Schmidt basis for $M = 2$. Meanwhile,

Lemma 12. *For $d = 2$ and $M \geq 4$, economical universal cloning is impossible.*

Proof. It is sufficient to prove that for $M = 4$ and $N \geq 12$ economical universal cloning is impossible, because if the partial trace of $|\Phi\rangle \langle \Phi|$ onto just four qubits does not give the projector onto the symmetric subspace, then the partial trace onto any larger number of qubits cannot give a projector onto the symmetric subspace (because that projector's partial trace would, itself, be a projector onto the symmetric subspace).

We write

$$|\Phi\rangle = \sum_{i=0}^{N-4} \alpha_i \left| \phi_i^{(N-4)} \right\rangle$$

where the states $|\phi_i^{(N-4)}\rangle$ are the uniform superpositions of i $|1\rangle$ states (a basis of the symmetric subspace of $N - 4$ qubits). We require that $\sum_i |\alpha_i|^2 = 1$ and that $\alpha_i \geq 0$ for all i (since the maximum eigenvector must have non-negative coefficients). Now examine the Schmidt decomposition of the states $|\phi_i^{(N-4)}\rangle$:

$$\left| \phi_i^{(N-4)} \right\rangle = \sum_{j=\max(0, i+8-N)}^{\min(i, 4)} \frac{\binom{4}{j} \binom{N-8}{i-j}}{\binom{N-4}{i}} \left| \phi_j^{(4)} \right\rangle \left| \phi_{i-j}^{(N-8)} \right\rangle.$$

So, if two terms α_i and α_k are non-zero ($i \neq k$), they yield an off-diagonal term in $\text{Tr}_{N-8} |\Phi\rangle \langle \Phi|$, as written in the basis of the symmetric states, whenever there exist j and l such that $i - j = k - l$ within their appropriate summation ranges. If such a term arises, at least

one of α_i, α_k must be 0 because we require the state to be diagonal in the symmetric basis. In particular, for $i = 4, \dots, N-8$, this imposes that $\alpha_i = 0$ because these states $|\phi_i\rangle$ give off-diagonal terms with every other possible state. Thus, to ensure a diagonal outcome, we either pick $\alpha_i = 0$ or all $\alpha_k = 0$ for $k \neq i$. In the latter case, it is easy to verify that $\text{Tr}_{N-8} |\phi_i\rangle \langle \phi_i| \neq P_{\text{sym}}^4$. A similar analysis continues between all the $i = 0, 1, 2, 3$, where we conclude that only one of them can be non-zero to ensure that the output is diagonal. And, again, for all the $i = N-8+1, \dots, N-4$. So, let us pick $i \in \{0, 1, 2, 3\}$ and $j \in \{N-7, N-6, N-5, N-4\}$ to be α_i and α_j are the only non-zero terms. What are the matrix elements of the $|0000\rangle \langle 0000|$ and $|1111\rangle \langle 1111|$ components of the reduced state of $|\Phi\rangle \langle \Phi|$?

$$|\alpha_i|^2 \frac{\binom{N-8}{i}}{\binom{N-4}{i}} \quad |\alpha_j|^2 \frac{\binom{N-8}{j-4}}{\binom{N-4}{j}},$$

both of which need to be $1/5$ in order to get the projector on the symmetric subspace. However, we also require the normalisation condition for $|\Phi\rangle$:

$$|\alpha_i|^2 + |\alpha_j|^2 = \frac{1}{5} \left(\frac{\binom{N-4}{i}}{\binom{N-8}{i}} + \frac{\binom{N-4}{j}}{\binom{N-8}{j-4}} \right) = 1.$$

By iterating through all possible values of i, j and solving the equation for N , we find that there is never an integer value of N that is a valid solution. \square

We are now in the position that, given a set $\{\alpha_x\}$, we can find the corresponding optimal cloning fidelities, simply by solving for the maximum eigenvector of an $\binom{N}{M} \times \binom{N}{M}$ matrix. However, being given the set α_x is an unnatural setting, and was merely a mathematical convenience. It would be far more useful to be able to either describe the region of achievable cloning fidelities and how they trade-off against each other, or to be able to ascertain whether a given set of fidelities are achievable.

The former question makes most sense when the possible fidelities are constrained. For example, if we consider the set of fidelities $\Lambda \subseteq \{0, 1\}^N$ by restricting to those strings of fixed Hamming weight, L . Instead of trying to find the maximum eigenvector as a function of $\{\alpha_x\}$ and eliminating them, we use the fidelities to eliminate the $\{\beta_x\}$ from the normalisation condition.

IV. FIDELITY RELATIONS: $N-1 \rightarrow N$ CLONING

When $M = N-1$, there is a single site at which a given bit string $x \in \{0, 1\}^N : w_x = N-1$ (referring to β_x) is 0. So, we choose (in this section only) to revise the notation to β_n where $x_n = 0$, while if $L = 1$ we use F_k to mean $y_k = 1$ (the only site at which y is not 0). The normalisation condition is

$$\left(\sum_n \beta_n \right)^2 + (d-1) \sum_n \beta_n^2 \leq d.$$

We will concentrate on the optimum achievable fidelities, and, as such, will take equality in the normalisation condition. The fidelities are given by

$$F_k = 1 - \frac{d-1}{d} \beta_k^2.$$

The manipulations are therefore particularly convenient,

$$N-1 = \sum_n F_n - \frac{1}{d-1} \left(\sqrt{1-F_n} \right)^2.$$

Moreover, for arbitrary L , we can readily find that

$$F_y = 1 - \frac{d-1}{d} \sum_{n:y_n=1} \beta_n^2 = \sum_{n:y_n=1} F_n - L + 1.$$

From any achievable set of single-copy fidelities, we can immediately derive the corresponding general fidelities:

$$F_y = y \cdot \underline{F} - w_y + 1$$

where \underline{F} is the vector of single-copy fidelities. Given an arbitrary set of fidelities, we solve for the set $\{F_n\}$

$$\min_{y \cdot \underline{F} \geq F_y + w_y - 1 \forall y \in \Lambda} \sum_n F_n - \frac{1}{d-1} \left(\sum_n \sqrt{1-F_n} \right)^2.$$

Cloning is possible if and only if this value is $\leq N-1$. We note that this is a convex optimisation problem – most obviously because the target function encapsulates the information from the positive definite matrix $G_0^{(M)}$ (that this is positive definite is clear because $G_0^{(M)}$ represents the Gram matrix of the vectors $|\psi_x\rangle$). Nevertheless, a full calculation of the eigenvalues is given in Appendix A). Since the problem is one of convex optimisation (see also Lemma 15), it can be efficiently solved by interior point methods²². Thus, the cloning problem can be resolved if $M = N-1$ for any set Λ .

V. $1 \rightarrow N$ CLONING

When $M = L = 1$, the bit strings have a single site at which there is a 1, so we replace $x \in \{0, 1\}^N : w_x = 1$ with a value $n \in [N]$. The normalisation condition reads

$$\left(\sum_n \beta_n \right)^2 + (d-1) \sum_n \beta_n^2 \leq d.$$

Each fidelity is calculated as

$$d(d+1)F_k = d + \left((d-1)\beta_k + \sum_n \beta_n \right)^2.$$

By summing over all k , we get that

$$\frac{d(d+1)}{N+d-1} \sum_k F_k = 2 \left(\sum_n \beta_n \right)^2 + (d-1) \sum_n \beta_n^2,$$

and we can rearrange the fidelity relation to give

$$(N + d - 1) \sum_n \beta_n = \sqrt{d} \sum_n \sqrt{F_n(d + 1) - 1}.$$

Eliminating these from the normalisation condition yields

$$\frac{(d + 1) \sum_n F_n}{N + d - 1} = 1 + \left(\frac{\sum_n \sqrt{F_n(d + 1) - 1}}{N + d - 1} \right)^2.$$

This describes the optimum trade-off between the asymmetric cloning fidelities. For example, if we set all the fidelities equal, we have

$$(N + d - 1)(d + 1)NF = (N + d - 1)^2 + N^2((d + 1)F - 1),$$

which rearranges to

$$F = \frac{2N + d - 1}{(d + 1)N},$$

the standard result on symmetric cloning. This cloning relation is equivalent to that found for the special case of $N = 3^7$, and was subsequently verified²³ for $N = 4^{24,25}$. A similar expression can be derived when $L = N - 1$, when the fidelities read

$$\binom{d + N - 3}{d - 1} F_k = \left(\sum_n \beta_n \right)^2 - \frac{2(d - 1)}{N - 1} \beta_k \sum_n \beta_n.$$

However, the final expression is rather too cumbersome to reproduce here.

A. Linear Constraints on Cloning

The essential feature of the derivations of optimal cloning fidelities for $M = 1, N - 1$ was the implicit ability to find linear combinations of the matrices $G_y^{(M)}$ and $G_0^{(M)}$ that are rank 1. This lets us reduce the quadratic constraints $\underline{\beta}^T G_y \underline{\beta} = F_y$ to linear ones on the $\{\beta_x\}$: if there exists a set of coefficients $\{g_y\}$ such that

$$g_0 G_0 + \sum g_y G_y = \underline{\Gamma} \cdot \underline{\Gamma}^T$$

where $\underline{\Gamma}$ is a unit vector, then

$$\underline{\Gamma}^T \underline{\beta} = \sqrt{g_0 + \sum g_y F_y}.$$

Lemma 13. *In $(1, L, N)$ cloning, there exist values $g_0, g_1, g_2 \in \mathbb{R}$ that yield a rank 1 projector*

$$P_1 = g_0 G_0 + g_1 G_{(1,0,0,\dots,0)}^{(M,L)} + g_2 G_0^{(M,L)}.$$

Proof. We observe that each of the 3 matrices $G_0, G_1^{(M,L)}, G_0^{(M,L)}$ has the form

$$\begin{aligned} G_0 &= \frac{1}{d}(|1\rangle + \sqrt{N - 1}|j\rangle)(\langle 1| + \sqrt{N - 1}\langle j|) + \frac{d - 1}{d} \mathbb{1} \\ G_1^{(M,L)} &= a_1 |1\rangle \langle 1| + a_2 (|1\rangle \langle j| + |j\rangle \langle 1|) + a_3 |j\rangle \langle j| + a_0 \mathbb{1} \\ G_0^{(M,L)} &= a_4 (|1\rangle + \sqrt{N - 1}|j\rangle)(\langle 1| + \sqrt{N - 1}\langle j|) + a_5 \mathbb{1} \end{aligned}$$

where $|j\rangle = \sum_{n=2}^N |n\rangle / \sqrt{N - 1}$ and we are using an index $n \in [N]$ in place of a bit string of length N with a single entry 1 at position n , and

$$\begin{aligned} a_0 &= a_2 - a_3 \\ a_1 &= \frac{\binom{N-1}{L-1}}{\binom{d+L-2}{d-1}} - a_0 \\ a_2 &= \frac{\binom{N-1}{L-1}}{N-1} \left(\frac{L-1}{\binom{d+L-2}{d-1}} + \frac{N-L}{\binom{d+L-1}{d-1}} \right) \\ a_3 &= \frac{\binom{N-1}{L-1}}{\binom{N-1}{2}} \left(\frac{\binom{L-1}{2}}{\binom{d+L-2}{d-1}} + \frac{(L-1)(N-L)}{\binom{d+L-1}{d-1}} + \frac{\binom{N-L}{2}}{\binom{d+L}{d-1}} \right) \\ a_4 &= \frac{\binom{N}{L}}{\binom{N}{2}} \left(\frac{\binom{L}{2}}{\binom{d+L-2}{d-1}} + \frac{L(N-L)}{\binom{d+L-1}{d-1}} + \frac{\binom{N-L}{2}}{\binom{d+L}{d-1}} \right) \\ a_5 &= \frac{\binom{N}{L}}{N} \left(\frac{L}{\binom{d+L-2}{d-1}} + \frac{N-L}{\binom{d+L-1}{d-1}} \right) - a_4. \end{aligned}$$

Any linear combination must also have the form of Eq. (4), such that by judicious choice of the parameters g , a rank 1 projector of the form $\underline{\Gamma} = \gamma_1 |1\rangle + \gamma_2 \sqrt{N - 1} |j\rangle$ results, where $\gamma_1 \neq \gamma_2$ and

$$\begin{aligned} \frac{g_0}{d} + g_1 a_1 + g_2 a_4 &= \gamma_1^2 \\ \frac{g_0}{d} + g_1 a_3 + g_2 a_4 &= \gamma_2^2 \\ \frac{d-1}{d} g_0 + a_5 g_2 + g_1 a_4 &= 0 \\ \gamma_1^2 + (N-1) \gamma_2^2 &= 1 \\ \left(\frac{g_0}{d} + g_1 a_2 + g_2 a_4 \right)^2 &= \gamma_1^2 \gamma_2^2. \end{aligned}$$

While the last condition may appear quadratic, provided $g_1 \neq 0$, this reduces to the linear one

$$g_0 \frac{a_1 + a_3 - 2a_2}{d} + g_1 (a_1 a_3 - a_2^2) + g_2 a_4 (a_3 - a_2) = 0.$$

It can only be the case that $\gamma_1 = \gamma_2$ if $a_1 = a_2$. This is equivalent to

$$a_2 = \frac{\binom{N-1}{L-1}}{\binom{d+L-2}{d-1}},$$

which further simplifies to

$$(N - L)(d - 1) = 0.$$

Hence, provided $L \neq N$ (whose solution is already known), we know that $\gamma_1 \neq \gamma_2$. \square

Consequently, we can write that

$$\gamma_2 \sum_{m=1}^N \beta_m + (\gamma_1 - \gamma_2) \beta_N = \sqrt{g_0 + g_1 \sum_{\substack{y \in \Lambda \\ y_1=1}} F_y + g_2 \sum_{y \in \Lambda} F_y}. \quad (5)$$

Given that $\gamma_1 \neq \gamma_2$, an equivalent but independent condition can be derived for each of the N sites (singling out a different β_n). By summing all of these, we get

$$((N-1)\gamma_2 + \gamma_1) \sum_m \beta_m = \sum_{n=1}^N \sqrt{g_0 + g_1 \sum_{\substack{y \in \Lambda \\ y_n=1}} F_y + g_2 \sum_{y \in \Lambda} F_y},$$

and hence we can calculate each of the individual β_n in terms of the fidelities. With the β_n in place, we simply have to verify if all the cloning fidelities, and the normalisation condition, are satisfied. For $L = 1, N - 1$, there are no outstanding quadratic conditions aside from normalisation, and the previous results are recovered.

For $1 < L < N - 1$, we consider our original problem, which can be phrased as the satisfiability problem

$$\begin{aligned} \min \quad & 1, \\ \text{subject to} \quad & \underline{\beta}^T G_0 \underline{\beta} = 1 \\ & \underline{\beta}^T G_y \underline{\beta} = \tilde{F}_y \quad \forall y \\ & \tilde{F}_y \geq F_y \quad \forall y \end{aligned}$$

where F_y are the target fidelities and the free parameters are the $\binom{N}{L}$ parameters β_n and the $\binom{N}{L}$ parameters \tilde{F}_y . By replacing the $\binom{N}{L}$ quadratic conditions with N linear ones (in β_n), just derived, the problem becomes convex, and hence efficiently solvable²² but misses out some of the constraints – satisfaction is necessary but not sufficient.

B. Consistency Relations

This situation can be improved by verifying the existence of consistency conditions between the fidelities. These will yield further linear relations that can be incorporated into the initial solution, meaning that there will only be $\binom{N}{2} - N$ quadratic constraints left to verify, independent of L (the forthcoming Lemma will return a space of $\binom{N}{2}$ quadratic constraints that need to be verified but Lemma 13 allows a further N to be removed).

Lemma 14. *Define the $\binom{N}{2} \times \binom{N}{L}$ matrix X as $\langle x | X | y \rangle = \delta_{x,y=2}$ where $x, y \in \{0, 1\}^N$ and $w_x = 2, w_y = L$. Any $\underline{v} \in \text{Ker}(X)$ satisfies $\sum_{y \in \Lambda} v_y G_y = 0$.*

Proof. We need to calculate both the diagonal

$$\langle n | \sum_{y \in \Lambda} v_y G_y | n \rangle = \frac{1}{\binom{d+L-1}{d-1}} \sum_{y \in \Lambda} v_y \left(1 + y_n \frac{d-1}{L} \right)$$

and off-diagonal, $\langle n | \sum_{y \in \Lambda} v_y G_y | m \rangle$:

$$\frac{1}{\binom{d+L}{d-1}} \sum_{y \in \Lambda} v_y \left(1 + (y_n + y_m) \frac{d-1}{L+1} + y_n y_m \frac{d(d-1)}{L(L+1)} \right)$$

matrix elements. Both are 0 due to the relations

$$\begin{aligned} \frac{1}{\binom{L}{2}} \sum_{x \in \{0,1\}^N: w_x=2} \langle x | X | v \rangle &= \sum_y v_y = 0 \\ \langle n, m | X | v \rangle &= \sum_y y_n y_m v_y = 0 \\ \frac{1}{L-1} \sum_{m \neq n} \langle n, m | X | v \rangle &= \sum_y y_n v_y = 0 \end{aligned}$$

since \underline{v} is in the Null space of X , and we have used $|n, m\rangle$ as a synonym for a weight-2 binary string where the 1s are at sites $n \neq m$. \square

Any optimal set of fidelities $\{F_y\}$, expressed as a vector \underline{F} , must satisfy $\underline{v} \cdot \underline{F} = 0$ for all $\underline{v} \in \text{Ker}(X)$, which yields $\binom{N}{L} - \binom{N}{2}$ independent conditions. We can therefore formulate our best solution to the cloning problem as a convex optimisation problem²² to satisfy

$$\begin{aligned} d(\gamma_1 - \gamma_2)^2 + (d-1) \left(N g_0 + \frac{N g_2}{L} q + g_1 q \right) &= \\ \frac{\sum_n \sqrt{g_0 + g_1 F_n + \frac{g_2}{L} q}}{((N-1)\gamma_2 + \gamma_1)^2} ((\gamma_1 - \gamma_2)^2 &- \\ - (d-1)\gamma_2(N\gamma_2 + 2(\gamma_1 - \gamma_2))) & \end{aligned}$$

(the normalisation condition) subject to the constraints

$$\begin{aligned} F_n &= \sum_{y: y_n=1} \tilde{F}_y \\ q &= \sum_{n=1}^N F_n \\ 0 &= \text{Ker}(X) \cdot \underline{\tilde{F}} \\ \tilde{F} &\geq \underline{F} \end{aligned}$$

This is a necessary condition for cloning – if it cannot be satisfied, cloning is impossible. If there is a satisfying assignment, then the β_n need to be derived so that the remaining conditions can be checked. If all are satisfied, cloning is possible, and the fidelities \tilde{F}_y are attained. If not, the question is unresolved. The remaining conditions do not appear to reduce to linear ones, but are readily specified. If we use $G_{a,b}^{(M,L)}$ as a synonym for $G_y^{(M,L)}$ when y is of weight 2, with $y_a = y_b = 1$ ($a \neq b$), and pick any 4 distinct sites ($N \geq 4$), then

$$\underline{\beta}^T (G_{a,b} + G_{c,d} - G_{a,c} - G_{b,d}) \underline{\beta} = \frac{2(d-1)(\beta_a - \beta_d)(\beta_b - \beta_c)}{(d+L)\binom{d+L-1}{d}}. \quad (6)$$

Recalling Eq. (5), we can easily evaluate terms such as $\beta_a - \beta_d$, and hence we have a whole new set of consistency conditions to verify. If we think of $F_{a,b} + F_{c,d} - F_{a,c} - F_{b,d}$ as an inner product $\underline{v}_{abcd} \cdot \underline{F}$, then one just has to pick $\frac{1}{2}N(N-3)$ linearly independent variants of \underline{v} , and all necessary conditions have been checked (this is the dimension of the space comprised of all possible vectors

\underline{v} , and is orthogonal to the vectors $\underline{\tilde{v}}$ for which $\underline{\tilde{v}} \cdot \underline{F} = F_n$). These conditions are non-convex.

To see that the main (normalisation) condition is convex, observe that for sufficiently large N , $1 - 2\sqrt{\alpha\gamma}d - (d-1)(N-2)\gamma$ is certainly negative, and

Lemma 15. *The function*

$$f_N(x) = \left(\sum_{n=1}^N \sqrt{x_n} \right)^2$$

is concave.

Proof. We use a proof by induction to show that $f_N(\alpha x + \beta z) \geq \alpha f_N(x) + \beta f_N(z)$. For the base case, we examine $N = 1$:

$$\left(\sqrt{\alpha x_1 + \beta z_1} \right)^2 \geq \alpha (\sqrt{x_1})^2 + \beta (\sqrt{z_1})^2,$$

which is straightforward.

Now we make the inductive step. Consider

$$f_N(\alpha x + \beta z) = \left(\sqrt{f_{N-1}(\alpha x + \beta z)} + \sqrt{\alpha x_N + \beta z_N} \right)^2,$$

assuming that $f_{N-1}(\alpha x + \beta z) \geq \alpha f_{N-1}(x) + \beta f_{N-1}(z)$. We simply need to show that the left-over terms are positive, i.e.

$$\begin{aligned} \sqrt{(\alpha x_N + \beta z_N) f_{N-1}(\alpha x + \beta z)} &\geq \\ \alpha \sqrt{f_{N-1}(x) x_N} + \beta \sqrt{f_{N-1}(z) z_N} \end{aligned}$$

Square the left-hand side, and again apply convexity. It would thus be sufficient to show that

$$\begin{aligned} (\alpha x_N + \beta z_N)(\alpha f_{N-1}(x) + \beta f_{N-1}(z)) &\geq \\ 2\sqrt{x_N z_N f_{N-1}(x) f_{N-1}(z)}, \end{aligned}$$

which is the same as

$$\left(\sqrt{x_N f_{N-1}(z)} - \sqrt{z_N f_{N-1}(x)} \right)^2 \geq 0,$$

which is clearly true. \square

VI. $2 \leq M \leq N - 2$ CLONING

For $M = 1, N - 1$, we can completely solve certain special values of L , and are left with only a modest number of constraints to verify in other cases (computationally, resolution of whether cloning is possible may still be a hard problem, but the more constrained it is, the more effectively we can witness the feasibility of cloning). However, for other values of M , there is no equivalent to Lemma 13.

Lemma 16. *For (M, L, N) cloning then if $N \leq 2M$ or M is even, and $N > M + 1$, there are no linear combinations*

$$P := g_0 + \sum_{y \in \Lambda} g_y G_y$$

which are non-trivial rank 1 projectors.

Proof. Central to our proof is the observation that for any 4 bit strings z_1 to z_4 of equal weight (M), if $z_1 \cup z_2 = z_3 \cup z_4$, then $\langle z_1 | P | z_2 \rangle = \langle z_3 | P | z_4 \rangle$ because it must be that $z_1 \cdot z_2 = z_3 \cdot z_4$ and $\bar{z}_1 \cap \bar{z}_2 = \bar{z}_3 \cap \bar{z}_4$.

Assume that $P = |v\rangle\langle v|$ for some vector $|v\rangle$. For any state $|\psi\rangle$, $P|\psi\rangle \propto |v\rangle$. Select two different basis states z_1, z_2 such that $\frac{1}{2}M \leq z_1 \cdot z_2 < M$. We know that

$$P|z_1\rangle \propto P|z_2\rangle.$$

However, look at a basis element $|x\rangle$ for which $\bar{x} \cdot (z_1 \oplus z_2) = 0$ (i.e. $x \cup z_1 = x \cup z_2$). By our observation, $\langle x | P | z_1 \rangle = \langle x | P | z_2 \rangle$. Hence, either $\langle x | P | z_1 \rangle = 0$ (i.e. either $P|x\rangle = 0$ or $P|z_2\rangle = 0$ for P to be rank 1) or $P(|z_1\rangle - |z_2\rangle) = 0$.

There must be at least one value z_1 for which $\langle v | z_1 \rangle \neq 0$, so start there. It is either that $\langle v | z_1 \rangle = \langle v | z_2 \rangle$, or $P|x\rangle = 0$ for all compatible x . Pick a specific x for which $x \cdot (z_1 \cup z_2) = M$ and $\bar{x} \cdot (z_1 \oplus z_2) = 0$. There is always at least one such x . This choice means that $z_1 \cup x = z_1 \cup z_2$ so that, by our observation,

$$\langle z_1 | P(|z_2\rangle - |x\rangle) = 0,$$

but now we know that $P|z_1\rangle \neq 0$ by assumption, so either $P|z_2\rangle = P|x\rangle = 0$ or $\langle v | z_1 \rangle = \langle v | z_2 \rangle = \langle v | x \rangle$. Ultimately, this propagates – either $\langle v | z_1 \rangle = \langle v | z_2 \rangle$ for all $z_2 : z_2 \cdot z_1 \geq \frac{1}{2}M$ or $P|z_2\rangle = 0$ for all $z_2 : \frac{1}{2}M \leq z_2 \cdot z_1 < M$.

However, we can now use our observation again. For any arbitrary z_2 , and the z_1 that we fixed, if M is even or $N \leq 2M$, there always exist z_3 and z_4 such that $z_1 \cup z_2 = z_3 \cup z_4$ and $z_1 \cdot z_3 \geq \frac{1}{2}M$, $z_1 \cdot z_4 \geq \frac{1}{2}M$ (If M is odd and $N > 2M$, then for $z_2 : z_1 \cdot z_2 = 0$, there are no suitable choices of z_3, z_4). The only possible solutions to this are that for some $t : w_x = K$ ($K \geq M$),

$$|v\rangle = \frac{1}{\sqrt{\binom{K}{M}}} \sum_{\substack{z: w_z=M \\ z \cdot t=M}} |z\rangle.$$

Of course, we already know that in the case of $N = M + 1$, it is possible to find linear combinations for which $K = M$ (i.e. a projector on a single basis state). So, we aim to show that this is impossible for larger values of N . Consider an arbitrary permutation π of the N -bit strings. If we take a sum of the relation

$$|v\rangle\langle v| = g_0 G_0 + \sum_y g_y G_y$$

over all such permutations, we find that

$$\frac{1}{\binom{N}{K}\binom{K}{M}} \sum_{x,z} |x\rangle \langle z| \binom{N-2M+x,z}{N-K} = g_0 G_0 + \frac{\sum_y g_y}{\binom{N}{M}} G_0^{(M,L)}.$$

All these matrices have matrix elements which depend only on the values $x \cdot z$, and we thus have a set of simultaneous equations

$$\frac{\binom{K-M}{M-q}}{\binom{N-M}{M-q}} = \frac{1}{\binom{M+d-1-q}{d-1}} \tilde{g}_0 + \frac{1}{\binom{2M+d-1-1}{d-1}} g_L$$

to be satisfied, for $q = \max(0, 2M - N) \dots M$. Note that, under the conditions of the theorem ($N > M + 1$ and $M \geq 2$), this means that there are at least 3 separate equations to satisfy, and only two free parameters to select, and thus cannot be solved in general. Indeed, since K only appears on the LHS of the equation, it must be that for any given M, N , there is no more than one compatible value of K . For simplicity, we have assumed that $L = M$, and have made the replacements $\tilde{g}_0 = \binom{N}{M} g_0$, $g_L = \binom{N+d-1}{M} \sum_y g_y$.

In the case where $N \leq 2M$, we start by considering the possibility that $K \leq 2M - 2$ (the choice of L is irrelevant here). In this case, $q = 2M - K - 1$ and $q = 2M - K - 2$ are both valid values, and mean that the left-hand side of the equation is 0 in both cases. Hence, $\tilde{g}_0 = g_L = 0$. This is clearly incompatible with any instance where the left-hand side is non-zero, such as $q = M$. Only the special cases of $K = N - 1, N$ remain. For $K = N$, take the cases $q = M, M - 1, M - 2$, and solve simultaneously between the equation pairs $M, M - 1$ and $M - 1, M - 2$ to derive two possible solutions for g_L . These are

$$\frac{g_L M}{d} = \binom{M+d}{d} = \binom{M+d-1}{d},$$

which are clearly never equal, so there is no satisfying assignment. The equivalent expression for $K = N - 1$ is

$$\begin{aligned} \frac{g_L M(d-1)(N-M)}{d \binom{M+d-1}{d}} &= \frac{M+d}{M} ((N-M)(d-1) - d) \\ &= (N-M-1)(d-1) - d - 1, \end{aligned}$$

which would require

$$d = \frac{N - 2M - 1}{N - M - 2},$$

but $d \geq 2$, so this cannot happen.

To analyse larger values of N , we first observe that our existing arguments automatically cover the case $K \leq 2M - 2$. We can thus restrict to the range $2M - 1 < K$. In a similar vein to before, we consider cases of q in pairs, but now it's $q = 0, 1$ and $q = 1, 2$, which we are assured exist due to $N > 2M$. We find that

$$\begin{aligned} g_L \frac{M(d-1) \binom{K-M}{M-1}}{\binom{N-M}{M-1} \binom{2M+d}{d}} &= (M+1) \left(\frac{K-2M+1}{N-2M+1} - \frac{M+d}{M+1} \right) \\ &= \frac{(2M+d+1)(M+2)}{2M+1} \left(1 - \frac{M+d+1}{M+2} \frac{N-2M+2}{K-2M+2} \right). \end{aligned}$$

This equality can be rewritten as

$$\frac{K-2M+2}{N-2M+1} \frac{2M+1}{2M+d+1} = 1 + \frac{N-M+d-1}{(M+d)(N-2M+1) - (M+1)(K-2M+1)}.$$

The left-hand side is clearly less than 1, while the right hand side is greater than 1. Satisfaction is impossible. \square

However, we do still benefit from a generalisation of Lemma 14.

Lemma 17. *Let $2M < L < N - 2M$. Define the $\binom{N}{2M} \times \binom{N}{L}$ matrix X as $\langle x|X|y\rangle = \delta_{x \cdot y = 2M}$ where $x, y \in \{0, 1\}^N$ and $w_x = 2M, w_y = L$. Any $\underline{v} \in \text{Ker}(X)$ satisfies $\sum_{y \in \Lambda} v_y G_y = 0$.*

Proof. Again, if $Y = \sum_{y \in \Lambda} v_y G_y$, then we must consider the diagonal, $\langle x|Y|x\rangle$ and off-diagonal elements $\langle x|Y|z\rangle$. We have that

$$\begin{aligned} \langle x|Y|x\rangle &= \sum_{q=0}^M \frac{1}{\binom{M+L+d-q-1}{d-1}} \sum_{y: y \cdot x = q} v_y \\ \langle x|Y|z\rangle &= \sum_{q=0}^{2M-x \cdot z} \frac{1}{\binom{M+L+d-q-1-x \cdot z}{d-1}} \sum_{y: y \cdot (x \cup z) = q} v_y, \end{aligned}$$

so all we need to know is that for all $q = 0, 1, \dots, 2M$, $\sum_{y: y \cdot x = q} v_y = 0$ when $x \in \{0, 1\}^N : w_x = q$. Pick any such x , then

$$\langle x|X|v\rangle = 0 = \sum_{y: x \cdot y = 2M} v_y$$

by definition. This proves a base case for induction. Now assume that

$$0 = \sum_{y: x \cdot y = q} v_y$$

for all $k+1 \leq q \leq 2M$, and we aim to prove it for the value k . Consider

$$\begin{aligned} 0 &= \sum_{\substack{z \in \{0,1\}^N \\ w_z = 2M \\ z \cdot x = k}} \langle z|X|v\rangle = \sum_{z: z \cdot x = k} \sum_{y: z \cdot y = 2M} v_y \\ &= \sum_{q=k}^{2M} \binom{2M}{k} \binom{N-2M}{2M-k} \binom{2M-k}{q-k} \binom{N-4M+k}{L-2M+k-q} \sum_{y: y \cdot x = q} v_y. \end{aligned}$$

Using our prior assumption, the desired result is clear, and we have proved the inductive step. \square

Hence, our general problem is reduced from $\binom{N}{L}$ quadratic constraints to $\binom{N}{2M}$ quadratic ones, with the difference being made up by linear constraints.

VII. COMPUTATIONAL COMPLEXITY OF CLONING

Ultimately, we would like to be able to answer the question “Given a set of fidelities $\{F_y\}$ for $y \in \Lambda \subseteq \{0, 1\}^N$, is cloning possible with these fidelities?”. This yes/no question lends itself to an analysis of its computational complexity. For any family of sets $\Lambda(N)$ for increasing N , a solution is easily verified – we can be given a proof in the form of a set of $\{\beta_x\}$, and all we have to do is verify the normalisation condition, and evaluate the achieved fidelities. The run time of such a check is polynomial in the size of the problem instance $|\Lambda|$. (Note that, unless M is finite, this does not necessarily mean that the run time is polynomial in N .) Thus, the problem is contained within the complexity class NP.

The fact that our computational problem is necessarily phrased as a non-convex optimisation problem suggests that it is a hard problem (assuming $P \neq NP$), and we conjecture that the problem is NP-complete, but have no proof. While the matrices of Eq. (6) are reminiscent of the matrices used in showing that rank 1 non-convex matrices can make a problem NP-hard²⁶, in fact it is not even clear that large N scaling is an interesting question, because we know that if all clones have to have non-trivial fidelities, the optimal strategy must tend towards the best classical strategy (measure and reproduce the measurement result) on all but a finite subset of the inputs and outputs (this is reminiscent of the behaviour emerging from the case study of $2 \rightarrow 4$ cloning of qubits in Appendix B). Of course, there may be subtleties of the attainable fidelities (the classical strategy is never strictly optimal), but these could easily lie at the limit of being so subtle as to be irrelevant. As such, the issue of computational complexity remains open.

VIII. QUANTUM CIRCUITS FOR ASYMMETRIC CLONING

Let us assume that we have found that a particular set of fidelities is achievable, and hence have a corresponding set of parameters $\{\beta_x\}$. How can we implement the cloning map? In principle, we know the unitary operation that we could implement – it’s specified in Lemma 11, but we don’t have an explicit circuit construction for it to show that it can be efficiently implemented.

Previously¹⁸, it has been suggested that the optimal cloner could be implemented by applying a superposition of different swap operations: start with the state $|B^{(M)}\rangle |\Phi\rangle$ and, with amplitude β_x , swap the spins 1 to M with those specified by the bit string x in order to produce $\sum_x \beta_x |B_x\rangle |\Phi\rangle_{\bar{x}}$. However, the construction of Wang et al.¹⁸ was only a sketch: it did not contain an efficiency analysis. Moreover, the implementation was necessarily probabilistic. This is inappropriate for quantum cloning because, with only one set of input states, there is no option to repeat until successful. For this reason, we do not give an explicit construction, but it is

closely related to the next construction.

In any case, a far better construction is to make the state $|\chi\rangle$ and to teleport the input states into the input spins. While this will use a similar technique to create the state, the advantage is that the probabilistic part of the algorithm can be allowed to fail as it doesn’t affect the state to be cloned, and can therefore be run using a repeat-until success strategy. The teleportation protocol runs as follows: one starts with the M input copies of state $|\psi\rangle$ on system IN' , and implements a Bell measurement on the symmetric subspaces of IN' and IN , i.e. projecting onto the basis

$$|\psi_{ab}\rangle = \frac{1}{\sqrt{\binom{M+d-1}{M}}} \sum_{i=0}^{\binom{M+d-1}{d-1}-1} \omega^{ia} |\phi_i^{IN'}\rangle |\phi_{i+b \bmod \binom{M+d-1}{M}}^{IN}\rangle$$

where $\omega = e^{2\pi i / \binom{M+d-1}{d-1}}$ and $a, b = 0, 1, \dots, \binom{M+d-1}{d-1} - 1$. If the result is $a = b = 0$, then the teleportation protocol works exactly as intended, and the clones appear on the output space OUT. Otherwise, a correction operation is required which maps states $\sum_x \beta_x \omega^{-ia} |\phi_{i+b \bmod \binom{M+d-1}{M}}^x\rangle |\Phi\rangle_{\bar{x}} \mapsto \sum_x \beta_x |\phi_i^x\rangle |\Phi\rangle_{\bar{x}}$. This is unitary by construction.

The required unitary is closely related to that for the unitary implementation of cloning and, as such, we do not have a general method for its implementation (or an efficiency analysis). However, for the special case of $M = 1$, the corrective gates are particularly simple (of course, we have already resolved that $M = 1, N - 1$ are the cases of primary interest for implementation, as these are the cases for which the asymmetry parameters can be determined). Each different Bell state projection effectively implements teleportation with a different single-qubit rotation applied to it (for $d = 2$, these are just the standard Pauli operators), and so the cloned states are just the ideal clones with those same rotations applied. They can therefore be removed by transversal application (i.e. simultaneous application to each of the N output spins) of the corresponding inverse operation. Indeed, for general M we can compensate for the different a answers in this way, although the b answers are not so easily compensated. However, even if we just proceeded to post-select on a $b = 0$ result, there would be a success probability of $1/\binom{M+d-1}{d-1}$, which is better than the success rate of the previous method.

To construct the desired state $|\chi\rangle$ (in fact, we will give the construction for the general case of non-economical cloning described in Corollary 4, using the mixed state), we first produce a state $|\chi_0\rangle$:

$$\frac{\sum_{i=0}^{\binom{M+d-1}{d-1}-1} \sum_{j=0}^{\binom{N-M+d-1}{d-1}-1} |\phi_i^{IN}\rangle |\phi_i^M\rangle |\phi_j^{N-M}\rangle |\phi_j^{N-M}\rangle}{\sqrt{\binom{M+d-1}{d-1} \binom{N-M+d-1}{d-1}}}$$

where the last set of $N - M$ spins are ancilla systems A that one should trace over to return the desired mixed

state (although keeping the ancillas is probably useful for applying the compensatory rotations to account for the different measurement results). This is easy since we can start from a GHZ-like state and can convert between computational basis states and symmetric states²⁷. Next, we need to produce a state

$$|\beta\rangle = \frac{\sum_x \beta_x |x_1\rangle |x_2\rangle |x_3\rangle \dots |x_M\rangle}{\sqrt{\sum_x \beta_x^2}},$$

where we use $|x_n\rangle$ to denote a set of $\lceil \log_2 N \rceil$ qubits containing a binary representation of the value m where the m th bit of x is the n th 1 in the string²⁸. For fixed M , since there are only $\binom{N}{M}$ terms β_x , the probability distribution β_x^2 can be efficiently integrated. Thus, $|\beta\rangle$ is easily constructed²⁹. Next, we take $|\beta\rangle |\chi_0\rangle$ and apply controlled-swaps controlled off the spins of the $|\beta\rangle$ system. In essence, if $|x_n\rangle$ takes value m then apply a swap between spins n and m of the output space in system $|\chi_0\rangle$. Therefore, we have produced the state

$$\frac{\sum_x \beta_x |x_1\rangle |x_2\rangle |x_3\rangle \dots |x_M\rangle}{\sqrt{\sum_x \beta_x^2}} \times \frac{\sum_{i=0}^{(M+d-1)-1} \sum_{j=0}^{(N-M+d-1)-1} |\phi_i^{\text{IN}}\rangle |\phi_i^x\rangle |\phi_j^{\bar{x}}\rangle |\phi_j^A\rangle}{\sqrt{\binom{M+d-1}{d-1} \binom{N-M+d-1}{d-1}}}.$$

Now we project all the $|\beta\rangle$ qubits onto the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. If successful, the output state is that desired,

$$\sum_x \beta_x \frac{\sum_{i=0}^{(M+d-1)-1} \sum_{j=0}^{(N-M+d-1)-1} |\phi_i^{\text{IN}}\rangle |\phi_i^x\rangle |\phi_j^{\bar{x}}\rangle |\phi_j^A\rangle}{\sqrt{\binom{M+d-1}{d-1} \binom{N-M+d-1}{d-1}}},$$

and this happens with a probability

$$\frac{1}{N^M \sum_x \beta_x^2}.$$

Since $1 = \sum_{x,z} \beta_x \beta_z / \binom{M+d-1-x \cdot z}{d-1} \geq \sum_x \beta_x^2$, this probability is no smaller than N^{-M} . For fixed M , we can therefore repeat on average a polynomial number of times in N and produce the target state.

IX. CONCLUSIONS

This paper has demonstrated necessary and sufficient conditions for optimal $1 \rightarrow N$ ($L = 1, N - 1$) and $N - 1 \rightarrow N$ universal cloning. In principle, these conditions can be used for bounding many-body correlations in a quantum system. We also explored why the cases of $2 \leq M \leq N - 2$ are more challenging – the conditions are necessarily formulated as non-convex constraints (whereas those that we have been able to solve can be reduced to linear constraints, which are consequently convex). We conjecture that, in such cases, the

cloning problem is NP-complete to resolve, and anticipate that the formulation provided in this paper should prove a suitable starting point for such studies of the computational complexity.

Appendix A: Matrix Properties

We study the spectral properties of the matrices $G_0^{(M)}$ which, while only tangentially relevant to the main text, may prove useful for future investigations.

Lemma 18. *For a fixed N , consider a matrix*

$$G^{(M)} = \sum_{x,z:w_x=w_z=M} f_{x \cdot z}^{(M)} |x\rangle \langle z|.$$

If

$$\tilde{\lambda} = \frac{(M+1-k)f_{k+1}^{(M+1)} + (N-2M-1+k)f_k^{(M+1)}}{(M+1-k)f_k^{(M)} + kf_{k-1}^{(M)}}$$

is independent of k and λ is an eigenvalue of $G^{(M)}$ of degeneracy g then $\lambda \tilde{\lambda}$ is an eigenvalue of $G^{(M+1)}$ with degeneracy g . If $N > 2M$, then there are $\binom{N}{M+1} - \binom{N}{M}$ additional (degenerate) eigenvalues given by

$$\frac{\binom{N}{M+1} f_{M+1}^{(M+1)} - \tilde{\lambda} \binom{N}{M} f_M^{(M)}}{\binom{N}{M+1} - \binom{N}{M}}.$$

Recursive calculation of the eigenvalues starts from $M = 0$ with a single eigenvalue of $f_0^{(0)}$.

Proof. Denote an eigenvector of $G^{(M)}$ of eigenvalue λ by $|\lambda^{(M)}\rangle = \sum_{y:w_y=M} \lambda_y |y\rangle$. We aim to prove that

$$|\lambda^{(M+1)}\rangle = \sum_{\substack{x \in \{0,1\}^N \\ w_x=M+1}} \sum_{\substack{y \in \{0,1\}^N \\ w_y=M \\ x \cdot y=M}} \lambda_y |x\rangle$$

is an eigenvector of $G^{(M+1)}$ of eigenvalue $\tilde{\lambda} \lambda$. If $|\lambda^{(M)}\rangle$ is an eigenvector of $G^{(M)}$ then for all y ($w_y = M$),

$$\lambda \lambda_y = \sum_{\tilde{x}:w_{\tilde{x}}=M} \lambda_{\tilde{x}} f_{\tilde{x} \cdot y}^{(M)}.$$

Selecting an x with $w_x = M + 1$, then

$$\lambda \sum_{\substack{y:w_y=M \\ x \cdot y=M}} \lambda_y = \sum_{\substack{y:w_y=M \\ x \cdot y=M}} \sum_{\tilde{x}:w_{\tilde{x}}=M} \lambda_{\tilde{x}} f_{\tilde{x} \cdot y}^{(M)}$$

Upon performing the sum over y first, we have to consider that the difference between the string x and any choice of y is a single site (which is a 1 for string x and a 0 for y), so there are $M + 1$ different strings y , but this means

that $x \cdot \tilde{x}$ and $y \cdot \tilde{x}$ must either be the same, or differ by 1. Hence,

$$\lambda \sum_{\substack{y:w_y=M \\ x:y=M}} \lambda_y = \sum_{\tilde{x}:w_{\tilde{x}}=M} \lambda_{\tilde{x}} \left((M+1-x \cdot \tilde{x}) f_{\tilde{x} \cdot x}^{(M)} + x \cdot \tilde{x} f_{\tilde{x} \cdot x-1}^{(M)} \right) \quad (\text{A1})$$

With this relation in place, we can proceed to look at the case of $M+1$. We need to prove that for all $x : w_x = M+1$,

$$\lambda \tilde{\lambda} \sum_{\substack{y:w_y=M \\ x:y=M}} \lambda_y = \sum_{z:w_z=M+1} \sum_{\substack{y:w_y=M \\ z:y=M}} f_{x \cdot z}^{(M+1)} \lambda_y$$

We reorder the two sums,

$$\begin{aligned} \text{RHS} &= \sum_{y:w_y=M} \sum_{\substack{z:w_z=M+1 \\ z \cdot y=M}} \lambda_y f_{x \cdot z}^{(M+1)} \\ &= \sum_{y:w_y=M} \lambda_y \left((M+1-x \cdot y) f_{x \cdot y+1}^{(M+1)} \right. \\ &\quad \left. + (N-2M-1+x \cdot y) f_{x \cdot y}^{(M+1)} \right) \end{aligned}$$

Provided $\tilde{\lambda}$ is independent of the value $k \equiv x \cdot y$, this is as desired.

When $N > 2M$, increasing the value of M increases the number of eigenvalues. If all the additional eigenvalues take on the same value, this value must be given by

$$\frac{\text{Tr}(G^{(M+1)}) - \tilde{\lambda} \text{Tr}(G^{(M)})}{\binom{N}{M+1} - \binom{N}{M}} = \frac{\binom{N}{M+1} f_{M+1}^{(M+1)} - \tilde{\lambda} \binom{N}{M} f_M^{(M)}}{\binom{N}{M+1} - \binom{N}{M}}$$

Proving that all the new eigenvalues are the same requires more careful consideration. Define the matrix

$$G_T = \sum_{x,z \in \{0,1\}^N} \delta_{w_x, w_z} f_{x \cdot z}^{(w_x)} |x\rangle \langle z| \equiv \bigoplus_{M=0}^N G^{(M)}.$$

Obviously, the different values of w_x (the separate $G^{(M)}$) define excitation subspaces, i.e. G_T commutes with the J_Z operator for N qubits. Furthermore, G_T is invariant under permutations of those N qubits: for a permutation π acting on bit strings, $(\pi x) \cdot (\pi z) = x \cdot z$. So, G_T also commutes with the total angular momentum operator J^2 , and we know it must therefore decompose into a structure of the form (given explicitly for even N^{30})

$$\bigoplus_{j=0}^{N/2} \mathcal{M}_j \otimes \mathbb{1}$$

where the $\mathbb{1}$ term associated with the index j is of dimension

$$\binom{N}{\frac{N}{2}-j} - \binom{N}{\frac{N}{2}-j-1}.$$

So, we can clearly identify the ‘new’ eigenvalues appearing for a particular value of $M = \frac{1}{2}N - j$ as being the

first instance of the \mathcal{M}_j subsystem (which populates the $w_x = \frac{1}{2}N - j$ to $\frac{1}{2}N + j$ excitation subspaces), and therefore have the correct degeneracy to all have the same eigenvalue. \square

Corollary 5. *The eigenvalues of matrix $G_0^{(M)}$ are*

$$\frac{\binom{d-2+k}{k} \binom{N+d-1}{M}}{\binom{M+d-1}{M} \binom{N+d-1}{k}} \quad k = 0, \dots, M$$

with degeneracy $\binom{N}{k} - \binom{N}{k-1}$.

Proof. With $f_k^{(M)} = \frac{1}{\binom{M+d-1-k}{d-1}}$, it turns out that $\tilde{\lambda} = \frac{N-M-1+d}{M+d}$, and the conditions of Lemma 18 are satisfied. \square

Corollary 6. *The inverse of $G_0^{(M)}$ is given by*

$$G_0^{-1} = \frac{(d+M-1)(N+d-M-1)}{(d-1)(d+N-1)} \sum_{x,z} \frac{(-1)^{M+x \cdot z} |x\rangle \langle z|}{\binom{d+N-2}{M-x \cdot z}}.$$

Proof. Again, the conditions of Lemma 18 hold, now with $\tilde{\lambda} = \frac{M+d-1}{N+d-2-M}$, the inverse of the scale factor for $G_0^{(M)}$. \square

Appendix B: A Case Study: $2 \rightarrow 4$ Cloning

We further illustrate the challenges involved in solving a case where $M \neq 1, N-1$ by examining in more detail the first such case, $2 \rightarrow 4$ cloning, using the two-copy fidelity measure $L=2$ on qubits, $d=2$ (The choice of $L=M$ can be anticipated to be the easiest to solve, as one would hope to find a one-to-one function between the $\{\beta_x\}$ and the $\{F_y\}$).

Let $x, y, z \in \{0,1\}^4$ be bit strings of weights $w_x = w_y = w_z = 2$, and let $\vec{\beta} = \sum_x \beta_x |x\rangle$ be a vector of real numbers. Lemma 16 has proven that there are no linear combinations of the matrices which are rank 1. However, if we further specialise by making the assumption that

$$F_y = F_{\bar{y}} \quad \forall y,$$

the task is significantly simplified. This means that we’re interested in exploring the cases of

$$\langle \beta | G_y - G_{\bar{y}} | \beta \rangle = 0 \quad \forall y. \quad (\text{B1})$$

Let’s introduce a basis change specified by

$$\tilde{H} = \frac{1}{\sqrt{2}} \sum_{\substack{x \in \{0,1\}^3 \\ w_x=1}} (|x1\rangle \langle x1| - |\bar{x}0\rangle \langle \bar{x}0| + |x1\rangle \langle \bar{x}0| + |\bar{x}0\rangle \langle x1|).$$

This gives, for example,

$$\tilde{H}G_0\tilde{H} = \frac{1}{30} \begin{pmatrix} 16 & 15 & 15 & 0 & 0 & 0 \\ 15 & 16 & 15 & 0 & 0 & 0 \\ 15 & 15 & 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

$$\tilde{H}(G_{0011} - G_{1100})\tilde{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \frac{2}{15} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} \\ 0 & 0 & 0 & 0 & -\frac{1}{10} & 0 \\ 0 & 0 & 0 & -\frac{1}{10} & 0 & 0 \\ \frac{2}{15} & \frac{1}{10} & \frac{1}{10} & 0 & 0 & 0 \end{pmatrix}.$$

One would anticipate that, given the assumption on symmetry of the fidelities, there'd be a similar symmetry in the $|\beta\rangle$ which, after the basis change manifests as $|\beta\rangle = (a, b, c, 0, 0, 0)^T$. It is certainly true that this form satisfies the three conditions of Eq. (B1), but there are other ways in which this can be achieved:

$$|\beta\rangle = \begin{cases} (-\frac{3}{4}(a+b), a, b, 0, 0, c)^T \\ (a, -\frac{3}{4}(a+b), b, 0, c, 0)^T \\ (a, b, -\frac{3}{4}(a+b), c, 0, 0)^T \end{cases}.$$

We have to try each of these cases in turn in order to assess which can achieve the largest fidelities, although the symmetry between these 3 cases means we only have to assess one of them. For now, we concentrate on the case $|\beta\rangle = (a, b, c, 0, 0, 0)^T$. We are therefore able to reduce to 3×3 matrices.

$$\langle \tilde{\beta} | \begin{pmatrix} 16 & 15 & 15 \\ 15 & 16 & 15 \\ 15 & 15 & 16 \end{pmatrix} | \tilde{\beta} \rangle = 30$$

$$\frac{22}{30} \langle \tilde{\beta} | \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} | \tilde{\beta} \rangle = 13(F_{1100} + F_{0011}) + 9$$

$$-9(F_{0101} + F_{1010} + F_{1001} + F_{0110})$$

So, we have the values for $|\tilde{\beta}\rangle = (a, b, c)^T$ and we can test if they satisfy the normalisation condition. We end up with the optimal condition

$$\sqrt{2(F_{1100} + F_{1010} + F_{0110}) - 1} = \sqrt{3} \sum_{\substack{x \in \{0,1\}^3 \\ w_x=2}} \sqrt{44F_{x0} - 18(F_{1100} + F_{1010} + F_{0110}) + 9}$$
(B2)

although there are constraints on the accessible values, since we require that, for example, $13(F_{1100} + F_{0011}) + 9 - 9(F_{0101} + F_{1010} + F_{1001} + F_{0110}) \geq 0$ because it corresponds to a squared quantity.

The above relation, depicted in Fig. 2, describes what, at first glance, might appear a surprising region – as one fidelity increases, the other fidelities also increase! However, this actually makes sense; if F_{0011} and F_{1100} are to

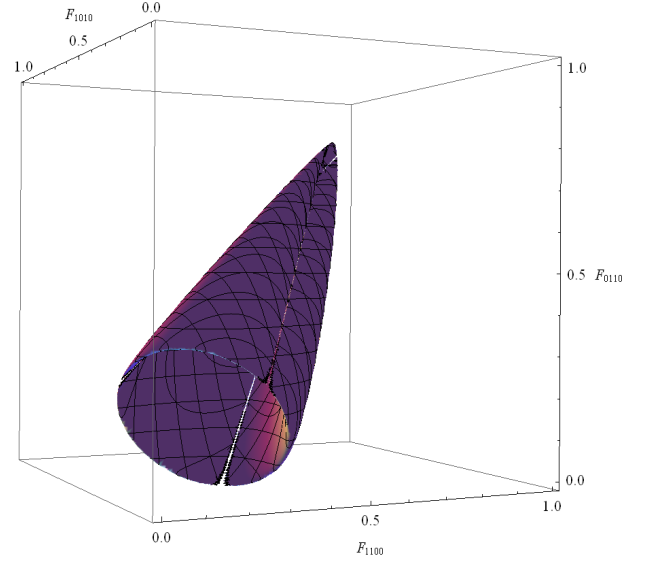


FIG. 2. Surface described by optimal cloning relation Eq. (B2).

both be high, they need a large component of an entangled state going from the two input spins to both qubit pairs (1, 2) and (3, 4), which automatically means that all fidelities must be high. In fact, it turns out that within this class of solutions, the fully symmetric point is a global maximum, i.e. there's no point in worrying about asymmetric cloning because the best result is to always implement fully symmetric cloning, and each of the fidelities is $\frac{61}{69}$.

We need to compare this to the case of $|\beta\rangle = (-\frac{3}{4}(a+b), a, b, 0, 0, c)^T$, from which we can derive a relation

$$(2F_{1010} + 2F_{0110} + 2 - 7F_{1100})(2F_{1010} + 2F_{0110} - 1 - F_{1100}) = \frac{9}{2}(F_{1010} - F_{0110})^2. \quad (\text{B3})$$

Again, we have positivity constraints:

$$\begin{aligned} 2F_{1010} + 2F_{0110} - 1 - F_{1100} &\geq 0 \\ 2F_{1010} + 2F_{0110} + 2 - 7F_{1100} &\geq 0 \\ 2F_{1010} + 2F_{0110} - 1 - \frac{5}{3}F_{1100} &\leq 0 \end{aligned}$$

We say that a set of cloning fidelities $\{F_{1100}, F_{1010}, F_{0110}\}$ can be achieved if there exists another set of fidelities $\{\tilde{F}_{1100}, \tilde{F}_{1010}, \tilde{F}_{0110}\}$ for which $\tilde{F}_x \geq F_x$ for all x , such that the \tilde{F}_x sit on the optimal cloning surfaces. The achievable fidelities are thus plotted in the final figure, where we see there are distinct phases of different cloning results, which is in stark contrast to the $1 \rightarrow N$ cloning that has been studied in the past in which there was no phase transition in the system as the cloning fidelities are varied.

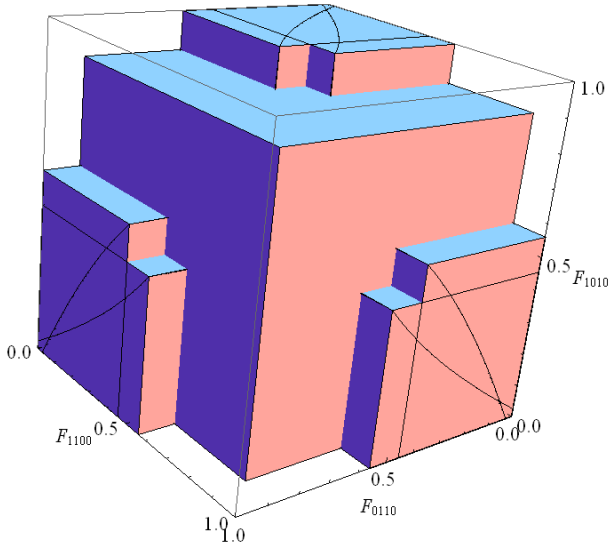


FIG. 3. Fidelity triples inside the shaded region can be achieved or exceeded.

REFERENCES

- ¹W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature* **299**, 802–803 (1982).
- ²V. Bužek and M. Hillery, “Quantum copying: Beyond the no-cloning theorem,” *Physical Review A* **54**, 1844–1852 (1996).
- ³R. F. Werner, “Optimal cloning of pure states,” *Physical Review A* **58**, 1827–1832 (1998).
- ⁴N. Gisin and S. Massar, “Optimal quantum cloning machines,” *Physical Review Letters* **79**, 2153 (1997).
- ⁵D. Bruss, A. Ekert, and C. Macchiavello, “Optimal universal quantum cloning and state estimation,” *Physical Review Letters* **81**, 2598–2601 (1998).
- ⁶V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, “Quantum cloning,” *Reviews of Modern Physics* **77**, 1225–1256 (2005).
- ⁷S. Iblisdir, A. Acín, N. J. Cerf, R. Filip, J. Fiuráscaronek, and N. Gisin, “Multipartite asymmetric quantum cloning,” *Physical Review A* **72**, 042328 (2005).
- ⁸S. Iblisdir, A. Acín, and N. Gisin, “Generalised asymmetric quantum cloning machines,” *Quantum Info. Comput.* **6**, 410–435 (2006).
- ⁹A. Kay, D. Kaszlikowski, and R. Ramanathan, “Optimal cloning and singlet monogamy,” *Physical Review Letters* **103**, 050501 (2009).
- ¹⁰A. Kay, R. Ramanathan, and D. Kaszlikowski, “Optimal asymmetric quantum cloning,” *Quantum Information & Computation* **13**, 880 (2013).
- ¹¹V. Coffman, J. Kundu, and W. K. Wootters, “Distributed entanglement,” *Physical Review A* **61**, 052306 (2000).
- ¹²T. J. Osborne and F. Verstraete, “General monogamy inequality for bipartite qubit entanglement,” *Physical Review Letters* **96**, 220503 (2006).
- ¹³R. Ramanathan, T. Paterek, A. Kay, P. Kurzyński, and D. Kaszlikowski, “Local realism of macroscopic correlations,” *Physical Review Letters* **107**, 060405 (2011).
- ¹⁴A. Jamiolkowski, “Linear transformations which preserve trace and positive semidefiniteness of operators,” *Reports on Mathematical Physics* **3**, 275–278 (1972).
- ¹⁵E. Lieb and D. Mattis, “Ordering energy levels of interacting spin systems,” *Journal of Mathematical Physics* **3**, 749–751 (1962).
- ¹⁶A. W. Harrow, “The church of the symmetric subspace,” arXiv:1308.6595 [quant-ph] (2013), arXiv: 1308.6595.
- ¹⁷M. Horodecki, P. Horodecki, and R. Horodecki, “General teleportation channel, singlet fraction, and quasidistillation,” *Phys. Rev. A* **60**, 1888–1898 (1999).
- ¹⁸Y. Wang, H. Shi, Z. Xiong, L. Jing, X. Ren, L. Mu, and H. Fan, “Unified universal quantum cloning machine and fidelities,” *Physical Review A* **84**, 034302 (2011).
- ¹⁹Roughly speaking, if a subset of a of size $\tilde{M} < M$ can be found as a subset of b , this corresponds conceptually to $\tilde{M} \rightarrow N$ cloning, which must be worse than $M \rightarrow N$ cloning.
- ²⁰T. Durt, J. Fiurásek, and N. J. Cerf, “Economical quantum cloning in any dimension,” *Physical Review A* **72**, 052322 (2005).
- ²¹D. Baguette, T. Bastin, and J. Martin, “Multiqubit symmetric states with maximally mixed one-qubit reductions,” *Physical Review A* **90**, 032314 (2014).
- ²²S. P. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).
- ²³At a time when Corollary 3 only had the status of a conjecture.
- ²⁴X. Ren, Y. Xiang, and H. Fan, “Optimal asymmetric $1 \rightarrow 4$ quantum cloning in arbitrary dimension,” *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics* **65**, 621–625 (2011).
- ²⁵P. Źwikliński, M. Horodecki, and M. Studziński, “Region of fidelities for a universal qubit quantum cloner,” *Physics Letters A* **376**, 2178–2187 (2012).
- ²⁶P. M. Pardalos and S. A. Vavasis, “Quadratic programming with one negative eigenvalue is NP-hard,” *Journal of Global Optimization* **1**, 15–22 (1991).
- ²⁷D. Bacon, I. L. Chuang, and A. W. Harrow, “The quantum schur and Clebsch-Gordan transforms: I. efficient qudit circuits,” in *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07 (Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2007) p. 1235–1244.
- ²⁸Subject to the small modification that any bits m in x which are 1 and $m \leq M$ must be specified as $x_m = m$. This avoids confusion when swapping different sites.
- ²⁹L. Grover and T. Rudolph, “Creating superpositions that correspond to efficiently integrable probability distributions,” arXiv:quant-ph/0208112 (2002), arXiv: quant-ph/0208112.
- ³⁰S. D. Bartlett, T. Rudolph, and R. W. Spekkens, “Reference frames, superselection rules, and quantum information,” *Reviews of Modern Physics* **79**, 555–609 (2007).